CA ARCserve® Replication and High Availability

Manuel d'installation

r15

Produits CA référencés

Ce document fait référence aux produits CA suivants :

- CA ARCserve® Replication
- CA ARCserve® High Availability (HA)
- CA ARCserve® Assured Recovery
- CA ARCserve® Content Distribution

Tout au long de ce manuel, le terme CA ARCserve RHA représente la famille de produits, préalablement appelée CA XOsoft Replication (WANsync) et CA XOsoft High Availability (WANsyncHA).

Informations de contact de CA

Pour une assistance technique en ligne et une liste complète des sites, horaires d'ouverture et numéros de téléphone, contactez le support technique à l'adresse http://www.ca.com/worldwide.

Table des matières

Chapitre 1 : Déploiement et composants de CA ARCserve RHA

Cette section présente les composants de CA ARCserve RHA et fournit des instructions permettant de déployer efficacement ces composants sur la plate-forme Microsoft Windows.

Ce chapitre traite des sujets suivants :

Composants de réplication et de haute disponibilité

CA ARCserve RHA inclut les composants suivants :

- Service de contrôle (page 9)
- Moteur (page 10)
- Centre de gestion (page 11) : inclut trois composants (page de présentation, gestionnaire et le centre de rapports)
- PowerShell (page 11)

service de contrôle

Le service de contrôle fonctionne en tant que point unique de contrôle lors de l'utilisation de la réplication ou de la haute disponibilité. Il contient la totalité de l'ensemble de données des scénarios existants et communique à la fois avec les moteurs et les gestionnaires. Il est chargé de gérer toutes les tâches liées aux scénarios, telles que la création, la configuration, la surveillance et l'exécution des scénarios.

Le service de contrôle reçoit les requêtes des gestionnaires, puis il les traite, les convertit en commandes et les transmet aux moteurs. Ceux-ci lui envoient ensuite des données et événements à jour. Le service de contrôle renvoie alors au gestionnaire des informations et des statistiques sur l'état du scénario.

Le service de contrôle est par ailleurs responsable de l'authentification et de l'autorisation des utilisateurs. Il peut en outre servir de point central pour le traitement et le stockage des rapports. L'utilisateur peut consulter les informations et statistiques recueillies par le service de contrôle au moyen de la page de présentation, du gestionnaire, du centre de rapports et du PowerShell.

Tous les fichiers de scénarios sont conservés sur le serveur exécutant le service de contrôle. Si le service de contrôle est arrêté, le fonctionnement du scénario n'est pas affecté. Toutefois, pour recevoir des informations sur l'état du scénario, le service de contrôle doit être actif. Pour obtenir de meilleurs résultats, installez le service de contrôle sur un hôte autonome. Si cela n'est pas possible, vous pouvez l'installer sur le serveur maître ou sur le serveur de réplication. Toutefois, si le serveur est arrêté, la connexion avec le service de contrôle est perdue et les scénarios ne sont plus gérables.

Vous pouvez protéger le service de contrôle CA ARCserve RHA dans des scénarios distincts. Pour plus d'informations, consultez la section Protection du service de contrôle dans le *Manuel d'administration de CA ARCserve RHA*.

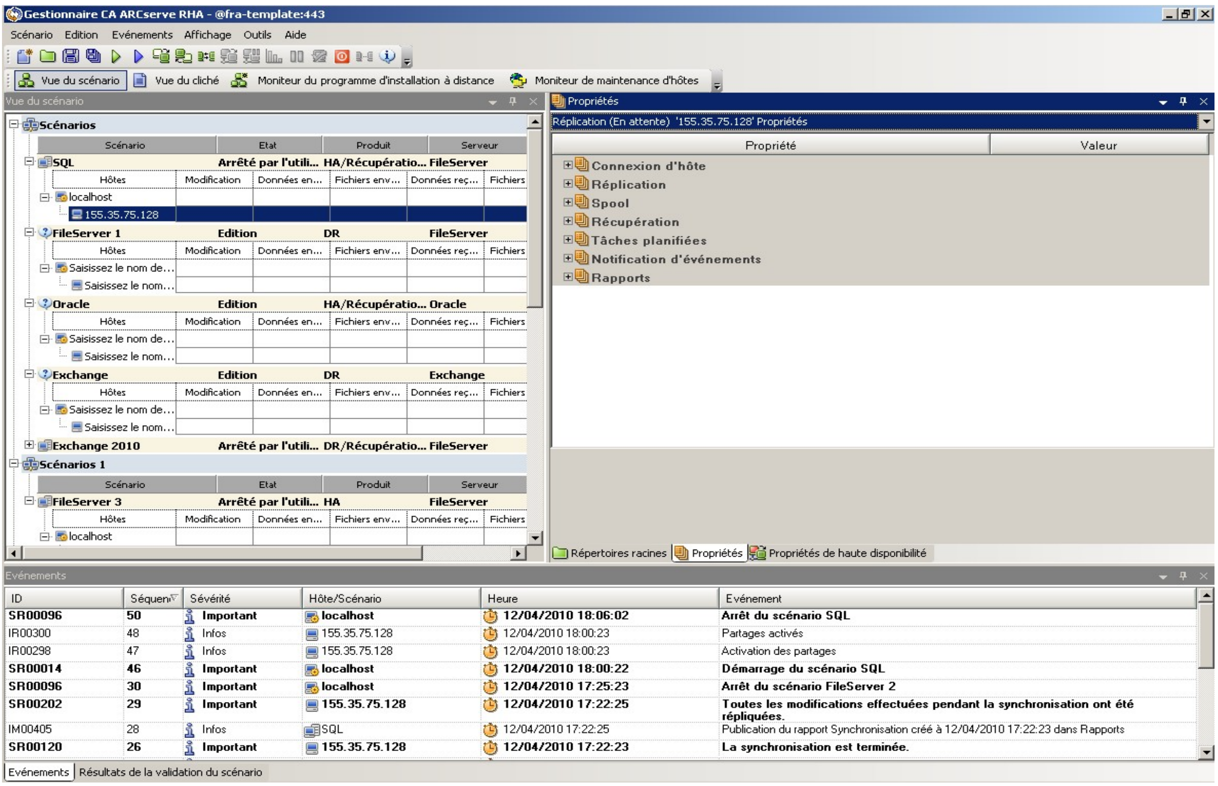
Moteur

Le moteur est un service Windows qui doit être en cours d'exécution pour qu'un scénario puisse être lancé. Il est installé sur tous les serveurs participant à un scénario, quel qu'il soit, c'est-à-dire les hôtes maîtres (source) et de réplication (cible). Chaque moteur prend en charge la fonctionnalité d'ordinateur maître et celle d'ordinateur de réplication, aussi bien pour les scénarios de récupération que pour ceux de haute disponibilité. Il peut participer à plusieurs scénarios et jouer un rôle différent dans chacun d'entre eux. Les moteurs peuvent être installés sur chaque hôte de façon locale, ou sur plusieurs hôtes à la fois via un programme d'installation distant, pendant la création d'un scénario, si nécessaire.

Centre de gestion

Le centre de gestion comprend trois composants, pour lesquels aucune installation manuelle n'est nécessaire.

- **Page de présentation** : aperçu statistique de l'état des scénarios de réplication et de haute disponibilité.
- **Gestionnaire** : interface utilisateur permettant de créer, de configurer, de gérer et de surveiller les scénarios. Cette interface utilisateur graphique s'active lorsque vous cliquez sur le lien Gestion des scénarios dans la page de présentation.



- **Centre de rapports** : interface utilisateur rassemblant tous les rapports existants, ainsi que des informations sur les rapports disponibles, par scénario. Vous pouvez choisir l'emplacement de stockage de ces rapports, ainsi que leur durée d'affichage et d'enregistrement dans le centre de rapports.

PowerShell

Le PowerShell est offert comme alternative à l'interface utilisateur graphique du gestionnaire pour les réplications. Ce composant étend et améliore les possibilités de l'interface de ligne de commande fournie avec les versions antérieures et prend en charge à la fois la réplication et la haute disponibilité.

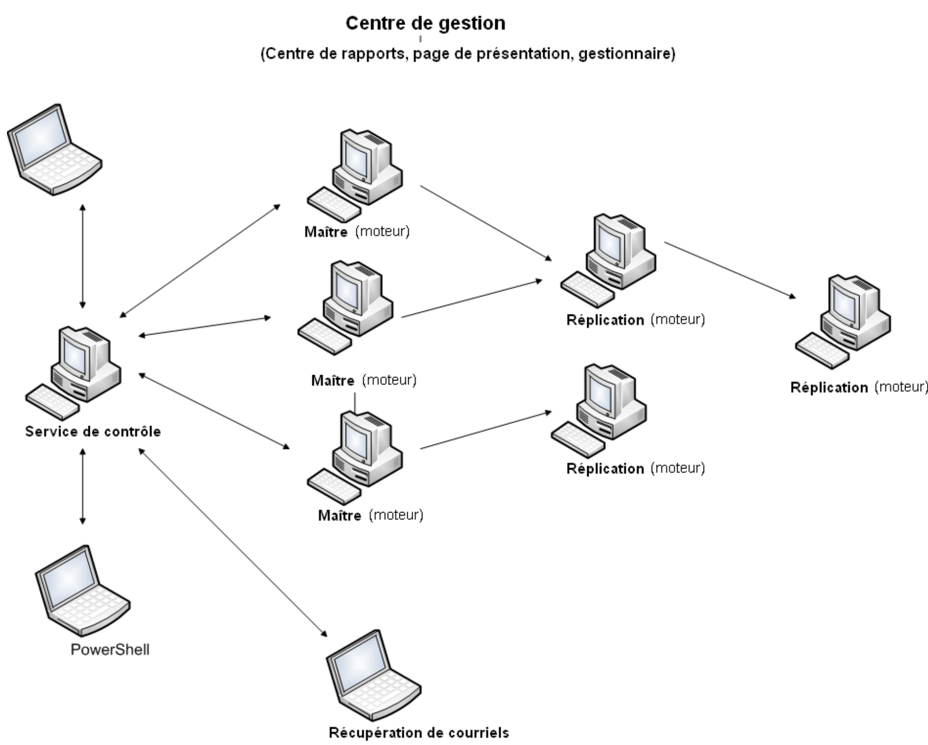
Le PowerShell est un shell de ligne de commande et un environnement de génération de scripts qui vous permet de configurer un scénario de réplication et de contrôler et surveiller le processus de réplication. Tous les scénarios gérés par le PowerShell ont une apparence et un fonctionnement identiques à ceux gérés par le gestionnaire. En outre, ils sont automatiquement enregistrés au même emplacement par défaut, à savoir répertoire_installation/ws_scenarios.

Le PowerShell se base sur l'interface standard Windows PowerShell™, fournie avec un ensemble étendu de commandes intégrées présentant la même interface. Le composant PowerShell offre plusieurs commandes supplémentaires liées au scénario (appelées des logiciels enfichables), qui facilitent la gestion des scénarios.

Déploiement de CA ARCserve RHA

Le déploiement des composants de CA ARCserve RHA dépend de la taille du réseau informatique de l'entreprise, ainsi que de vos besoins en matière de réplication et de haute disponibilité. Vous devez toutefois suivre certaines instructions lorsque vous concevez votre environnement de réplication et de haute disponibilité, et que vous déployez les différents composants sur une plate-forme Windows. La section suivante fournit des informations pour un déploiement efficace des composants de CA ARCserve RHA.

Le schéma suivant illustre le déploiement habituel des composants de CA ARCserve RHA :



- **Service de contrôle CA ARCserve RHA**

  Le service de contrôle doit pouvoir se connecter à tous les serveurs maîtres et à tous les serveurs de réplication exécutant la permutation. Il ne doit pas nécessairement établir de connexion directe avec chacun des serveurs de réplication sans permutation dans les scénarios.

  Nous vous recommandons d'installer le service de contrôle sur un serveur à part. Si vous utilisez des scénarios de haute disponibilité, n'installez le service de contrôle ni sur l'hôte maître, ni sur l'hôte de réplication.

  Vous pouvez installer le service de contrôle sur votre station de travail locale. Notez toutefois que si cette station de travail est désactivée ou hors ligne, vous ne pourrez ni surveiller, ni gérer vos scénarios.

- **Moteur CA ARCserve RHA**

  Le moteur doit être installé sur chaque serveur maître et chaque serveur de réplication participant aux scénarios définis.

- **Centre de gestion CA ARCserve RHA**

  Vous pouvez ouvrir ce composant à partir de n'importe quelle station de travail dotée d'un navigateur et d'une connexion réseau au service de contrôle.

- **PowerShell pour CA ARCserve RHA**

  Vous pouvez ouvrir ce composant à partir de n'importe quelle station de travail dotée de Windows PowerShell et d'une connexion réseau au service de contrôle.

Chapitre 2 : Configurations et conditions requises pour les composants CA ARCserve RHA

Cette section fournit des informations relatives au logiciel et aux configurations requises pour chaque composant CA ARCserve RHA.

Remarque : Pour obtenir la liste actualisée des systèmes d'exploitation pris en charge, reportez-vous au document Notes de parution ou consultez le site Web de CA, à l'adresse arcserve.com.

Ce chapitre traite des sujets suivants :

Configuration requise pour le service de contrôle

Systèmes d'exploitation

- Windows Server 2008 32 bits et 64 bits R2
- Windows 2003 Server

Remarque: Pour éviter des erreurs de configuration de Microsoft, installez le service de contrôle sur les systèmes Windows Server 2003 et Windows Server 2008 R2 en utilisant le compte d'administrateur si vous envisagez de déployer le moteur sur des hôtes locaux au moyen du programme d'installation à distance.

Important : Pendant l'installation du service de contrôle, lorsque vous entrez les informations de connexion au service, vous pouvez utiliser un compte d'administrateur ou définir un nouveau compte. Si vous définissez un nouveau compte, activez l'état de démarrage du service Explorateur d'ordinateurs du système d'exploitation et vérifiez que le service est en cours d'exécution. Sur Windows 2003, le service Explorateur d'ordinateurs est activé par défaut. En revanche, sur Windows Server 2008, l'état de démarrage du service Explorateur d'ordinateurs est **désactivé** par défaut. Par conséquent, pour installer le service de contrôle sur Windows 2008 et définir un nouveau compte système associé, avant de commencer l'installation, vous devez définir l'état de démarrage du service Explorateur d'ordinateurs sur **Automatique**, et démarrez le service. Le service Explorateur d'ordinateurs repose sur le partage de fichiers et d'imprimantes : vous devrez également activer le **partage de fichiers et d'imprimantes** dans le centre Réseau et partage. Pour plus d'informations sur l'activation de l'état de démarrage du service Explorateur d'ordinateurs, reportez-vous à la page : http://technet.microsoft.com/en-us/library/bb726965.aspx.

Une fois l'installation terminée, vous pouvez arrêter le service Explorateur d'ordinateurs et redéfinir son état de démarrage sur **Désactivé**.

Plusieurs applications requises sont installées automatiquement sur votre ordinateur au cours de l'installation, si elles ne le sont pas déjà. Ces applications sont les suivantes.

- Microsoft .NET Framework Version 2.0
- Microsoft ASP.NET 2.0 AJAX Extensions 1.0
- Microsoft Core XML Services 6.0
- Microsoft SQL Server Management Objects Collection
- Microsoft SQL Server Native Client

Informations d'identification de l'utilisateur

- Un utilisateur Windows exécutant le service de contrôle CA ARCserve RHA requiert une autorisation d'accès au répertoire d'installation en lecture et en écriture.

Configuration requise pour le moteur

Le composant Moteur s'exécute sous les systèmes d'exploitation suivants.

- Windows Server 2008, 2008 R2 32 bits et 64 bits
- Windows Server 2003
- AIX
- Solaris
- Red Hat Linux
- SUSE Linux

Important : Pendant l'installation du moteur, lorsque vous entrez les informations de connexion au service, vous pouvez utiliser un compte système local ou définir un nouveau compte. Si vous définissez un nouveau compte, activez l'état de démarrage du service Explorateur d'ordinateurs du système d'exploitation et vérifiez que le service est en cours d'exécution. Sur Windows 2003, le service Explorateur d'ordinateurs est activé par défaut. En revanche, sur Windows Server 2008, l'état de démarrage du service Explorateur d'ordinateurs est **désactivé** par défaut. Par conséquent, pour installer le moteur sur Windows 2008 et définir un nouveau compte système associé, avant de commencer l'installation, vous devez définir l'état de démarrage du service Explorateur d'ordinateurs sur **Automatique**, et démarrez le service. Le service Explorateur d'ordinateurs repose sur le partage de fichiers et d'imprimantes : vous devrez également activer le partage de fichiers et d'imprimantes dans le centre Réseau et partage. Pour plus d'informations sur l'activation de l'état de démarrage du service Explorateur d'ordinateurs, reportez-vous à la page : http://technet.microsoft.com/en-us/library/bb726965.aspx.

Une fois l'installation terminée, vous pouvez arrêter le service Explorateur d'ordinateurs et redéfinir son état de démarrage sur **Désactivé**.

Configuration requise pour le centre de gestion

Navigateur Web

- Internet Explorer 6, 7 ou 8

Compte de connexion

- Pour vous connecter au centre de gestion, vous devez être un membre du groupe d'administrateurs de l'ordinateur local où le service de contrôle est installé.

Configuration requise pour PowerShell

Systèmes d'exploitation

- Windows Server 2008 32 bits et 64 bits
- Windows Vista
- Windows Server 2003
- Windows XP

.Net Framework

- Microsoft .NET Framework 2.0 (compilation 50727)

Pour l'installation de Windows PowerShell, .Net Framework est nécessaire. Vous pouvez le télécharger et l'installer à partir du Centre de téléchargement Microsoft.

Microsoft PowerShell

- Microsoft PowerShell version 1.0

L'application PowerShell est intégrée à Windows Vista SP1. Si vous utilisez Windows XP ou 2003, vous pouvez la télécharger et l'installer directement à partir de Microsoft.

Chapitre 3 : Configuration requise pour les applications et bases de données prises en charge

Cette section fournit des informations sur les configurations et les conditions de comptes de connexion de chaque serveur d'application et de base de données pris en charge et de chaque solution de réplication.

Remarque : Les configurations et les conditions requises pour un serveur de fichiers sont décrites à la section Installation du moteur CA ARCserve RHA (page 63).

Ce chapitre traite des sujets suivants :

Serveurs d'applications et de bases de données pris en charge

Les solutions de réplication et de haute disponibilité sont adaptées aux serveurs de bases de données et d'applications suivants, avec Windows 32 bits ou 64 bits.

- Serveur de fichiers
- Microsoft Exchange
- Microsoft SQL
- Microsoft IIS
- Oracle
- Microsoft SharePoint
- Microsoft Hyper-V
- VMware vCenter Server
- Service de contrôle CA ARCserve RHA
- Microsoft Dynamics CRM

CA ARCserve RHA peut également transférer des systèmes complets vers des ordinateurs virtuels. Pour obtenir la liste actualisée des plates-formes et des applications prises en charge, reportez-vous au document *CA ARCserve RHA Supported Configurations* (configurations prises en charge par CA ARCserve RHA) sur le site Web de support de CA.

Important : Pour tous les serveurs pris en charge, vous devez affecter statistiquement toutes les adresses IP (les adresses IP DHCP sur le serveur maître ou le serveur de réplication ne sont pas prises en charge).

Haute disponibilité et réplication pour serveurs de fichiers

Cette section décrit les conditions requises pour l'exécution de CA ARCserve RHA pour les serveurs de fichiers.

Configuration requise pour le serveur de fichiers

Pour implémenter les procédures de haute disponibilité pour le serveur de fichiers, vous devez disposer des configurations ci-dessous.

- Deux serveurs exécutant Windows Server 2003 ou 2008
- Les deux serveurs doivent résider dans la même forêt Active Directory et être membres du même domaine ou de domaines sécurisés.
- Affectez statiquement toutes les adresses IP. Les adresses IP affectées par le serveur DHCP sur le serveur maître ou de réplication ne sont pas prises en charge.
- Le serveur protégé n'est pas un contrôleur de domaine ou un serveur DNS.

Compte de connexion pour le serveur de fichiers

Le compte de connexion au service CA ARCserve HA doit remplir toutes les conditions de compte ci-dessous.

- Il est membre du groupe Administrateurs de domaine. Si le groupe Administrateurs de domaine n'est pas membre des administrateurs du groupe local de domaine intégré, vous devez utiliser un compte qui le soit.
- Il est membre du groupe d'administrateurs de l'ordinateur local. Si le groupe Administrateurs de domaine n'est pas membre, ajoutez le compte manuellement.

Serveurs de fichiers fonctionnant dans un groupe de travail

Pour les serveurs d'un groupe de travail, définissez le compte de service du moteur CA ARCserve RHA sur Système local (sauf si vous avez ajouté des scripts personnalisés qui requièrent des niveaux d'autorisation plus élevés). Les serveurs d'un groupe de travail peuvent utiliser la redirection du système DNS uniquement avec les serveurs DNS qui autorisent les mises à jour non sécurisées. Vous pouvez utiliser normalement le transfert IP, la permutation du nom de l'ordinateur et les scripts de redirection personnalisés.

Réplication et haute disponibilité pour Microsoft Exchange Server

Cette section décrit la configuration requise de CA ARCserve RHA pour Microsoft Exchange Server.

Réplication pour serveurs Exchange

Cette section décrit les conditions requises pour l'exécution de CA ARCserve RHA pour les serveurs Exchange.

Configuration de la réplication pour serveurs Exchange

Pour implémenter la réplication pour un serveur Exchange, les configurations suivantes sont nécessaires :

- Deux serveurs exécutant Windows Server 2003 ou 2008
- Le serveur Exchange est installé à la fois sur les serveurs maître et de réplication, qui comprennent les mêmes éditions, versions, Services Packs et correctifs.
- Le serveur Exchange doit être installé avec les mêmes informations d'identification sur les serveurs maître et de réplication.
- Les rôles CAS et la boîte aux lettres doivent être installés sur les deux serveurs. Si le serveur maître est le seul serveur dans l'organisation Exchange qui comprend les rôles de transfert CAS et HUB, alors le serveur de réplication doit disposer des mêmes rôles que le serveur Exchange.
- Les mêmes versions de PowerShell doivent être installées sur les deux serveurs.
- Les deux serveurs doivent inclure le même groupe administratif Exchange.

Remarque: Le serveur Exchange 2010 ne vous permet pas de créer deux bases de données avec le même nom sur les serveurs maître et de réplication, même si la base de données est démontée. Utilisez un nom pour la base de données de réplication ne dépassant pas 64 caractères et suivez cette convention :

<nom_réplication>=<nom_maître>_xxxx

Où xxx = nombre aléatoire

Compte de connexion pour la réplication Exchange

Le compte de connexion au service du moteur CA ARCserve RHA doit remplir toutes les conditions suivantes :

- Il doit s'agir d'un Administrateur Exchange - Affichage seul.
- Il doit être membre du groupe Administrateurs sur l'ordinateur local.

Remarque : Si la stratégie de sécurité de votre société nécessite des autorisations plus précises que celles décrites, contactez le support technique CA pour obtenir des instructions détaillées sur les autorisations requises.

Clusters de réplication Exchange

Avec CA ARCserve RHA, l'utilisation de clusters est similaire à l'utilisation de serveurs autonomes. Il vous suffit de saisir le nom du serveur Exchange virtuel comme nom de serveur maître ou de serveur de réplication le cas échéant.

Sur Exchange 2007, CA ARCserve RHA prend en charge les déploiements LCR. Aucune configuration supplémentaire n'est nécessaire.

Remarque : Sur Exchange 2007, les déploiements CCR ne sont pas pris en charge.

Haute disponibilité pour serveur Exchange

Cette section décrit la configuration requise pour exécuter CA ARCserve HA sur un serveur Exchange.

Configuration de la haute disponibilité pour Exchange

Pour implémenter la réplication pour un serveur Exchange, les configurations suivantes sont nécessaires :

- Deux serveurs exécutant Windows Server 2003 ou 2008
- Le serveur Exchange est installé à la fois sur les serveurs maître et de réplication, qui comprennent les mêmes éditions, versions, Services Packs et correctifs.
- Le serveur Exchange doit être installé avec les mêmes informations d'identification sur les serveurs maître et de réplication.
- Les rôles CAS et la boîte aux lettres doivent être installés sur les deux serveurs. Si le serveur maître est le seul serveur dans l'organisation Exchange qui comprend les rôles de transfert CAS et HUB, alors le serveur de réplication doit disposer des mêmes rôles que le serveur Exchange.
- Les mêmes versions de PowerShell doivent être installées sur les deux serveurs.
- Les deux serveurs doivent inclure le même groupe administratif Exchange.

Remarque: Le serveur Exchange 2010 ne vous permet pas de créer deux bases de données avec le même nom sur les serveurs maître et de réplication, même si la base de données est démontée. Utilisez un nom pour la base de données de réplication ne dépassant pas 64 caractères et suivez cette convention :

<nom_réplication>=<nom_maître>_xxxx

Où xxx = nombre aléatoire

Compte de connexion pour la haute disponibilité d'Exchange

Le compte de connexion au service du moteur CA ARCserve HA doit remplir toutes les conditions ci-dessous.

- Il doit être membre du groupe Administrateurs de domaine.
- Il doit être Administrateur Exchange.
- Il doit être membre du groupe Administrateurs sur l'ordinateur local.

Remarque : Si la stratégie de sécurité de votre société requiert des autorisations plus précises que celles décrites, contactez le support technique de CA ARCserve RHA pour obtenir des instructions détaillées sur les autorisations requises.

Clusters de haute disponibilité pour serveurs Exchange

Avec CA ARCserve HA, l'utilisation de clusters est presque similaire à l'utilisation de serveurs autonomes. Il vous suffit de saisir le nom du serveur Exchange virtuel comme nom de serveur maître ou de serveur de réplication le cas échéant.

Sur Exchange 2007, CA ARCserve HA prend en charge les déploiements LCR. Aucune configuration supplémentaire n'est nécessaire.

Remarque : Sur Exchange 2007, les déploiements CCR (Cluster Continuous Replication, réplication continue en cluster) ne sont pas pris en charge.

Réplication et haute disponibilité pour Microsoft SQL Server

Cette section décrit les conditions requises pour CA ARCserve RHA pour Microsoft SQL Server.

Réplication pour SQL Server

Cette section décrit les conditions requises pour l'exécution de CA ARCserve RHA pour SQL Server.

Configuration de la réplication pour SQL

Pour implémenter la réplication pour SQL Server, les configurations suivantes sont nécessaires :

- Deux serveurs exécutant Windows Server 2003 ou 2008
- Une instance de SQL Server installée sur l'ordinateur maître

Pour utiliser la solution de réplication avec l'option de **récupération garantie** pour SQL Server, vous devez disposer des configurations suivantes.

- La même version de Microsoft SQL Server doit être installée sur les serveurs maître et de réplication.
- SQL Server doit être installé avec les mêmes informations d'identification sur les serveurs maître et de réplication.

Par ailleurs, vous devez arrêter le service SQL Server sur un hôte de réplication lorsque la réplication est active.

Remarque : Si la base de données maîtresse SQL n'est pas répliquée, vous pouvez détacher les bases de données répliquées sur le serveur de réplication sans arrêter le service du moteur.

Compte de connexion pour la réplication SQL

Le compte de connexion au service du moteur CA ARCserve RHA doit remplir toutes les conditions suivantes :

- Pour les serveurs autonomes (c'est-à-dire ceux qui ne sont pas en cluster), utilisez le compte par défaut du système local.
- Pour les noeuds de cluster, utilisez un compte de service ayant le rôle d'administrateur local sur tous les noeuds de cluster.

Haute disponibilité pour serveurs SQL

Cette section décrit la configuration requise pour exécuter CA ARCserve HA sur un serveur SQL.

Configuration de la haute disponibilité de SQL

Pour implémenter les procédures de haute disponibilité du serveur SQL, vous devez disposer des configurations suivantes.

- Deux serveurs exécutant Windows Server 2003 ou 2008
- Une ou plusieurs instances de Microsoft SQL Server 2005 installées sur chaque serveur :
  - Les deux serveurs doivent disposer de la même version de SQL, des mêmes Service Packs et des mêmes correctifs.
  - Les deux serveurs doivent disposer d'instances SQL Server identiques, à savoir des instances par défaut ou nommées.
  - Les lettres du lecteur contenant les fichiers de base de données doivent être identiques sur les deux serveurs.
  - Le chemin complet de la base de données système par défaut pour chaque instance doit être identique sur les deux serveurs.
  - Les deux serveurs doivent résider dans la même forêt Active Directory et être membres du même domaine ou de domaines sécurisés.
- Vérifiez que le port défini dans les propriétés TCP/IP de la configuration réseau de la ou des instances SQL est affecté statiquement et qu'il est identique sur l'ordinateur maître et sur l'ordinateur de réplication
- Le serveur protégé n'est pas un contrôleur de domaine ou un serveur DNS.

Compte de connexion pour la haute disponibilité de SQL

Le compte de connexion au service du moteur CA ARCserve HA doit remplir toutes les conditions ci-dessous.

- Il est membre du groupe Administrateurs de domaine. Si le groupe Administrateurs de domaine n'est pas un membre du groupe local de domaines intégré Administrateurs, vous devez utiliser un compte qui soit membre de ce groupe.
- Il est membre du groupe d'administrateurs de l'ordinateur local. Si le groupe Administrateurs de domaine n'est pas membre, ajoutez le compte manuellement.
- Si le compte ne dispose pas d'autorisations d'administration intégrées sur toutes les instances SQL Server, ajoutez les autorisations adéquates.

Remarque : Si la stratégie de sécurité de votre société nécessite des autorisations plus précises que celles décrites, contactez le support technique pour obtenir des instructions détaillées. Pour les serveurs d'un groupe de travail, laissez l'utilisateur de la connexion comme système local.

Serveurs SQL fonctionnant dans un groupe de travail

Pour les serveurs d'un groupe de travail, définissez le compte de service du moteur CA ARCserve HA pour un utilisateur membre du groupe d'administrateurs locaux. Les serveurs d'un groupe de travail peuvent utiliser la redirection du système DNS uniquement avec les serveurs DNS qui autorisent les mises à jour non sécurisées. Vous pouvez utiliser normalement le transfert IP, la permutation du nom de l'ordinateur et les scripts de redirection personnalisés.

Clusters de haute disponibilité pour SQL

Pour une installation sur un cluster, saisissez le nom du serveur virtuel SQL Server comme nom du serveur maître ou de réplication.

L'utilisation du transfert IP avec un cluster est la seule configuration nécessitant une préparation. Pour obtenir des instructions détaillées sur l'utilisation du transfert IP avec des clusters, consultez le *Manuel des opérations pour Microsoft SQL Server CA ARCserve RHA*.

Haute disponibilité du serveur IIS

Cette section décrit la configuration requise pour exécuter CA ARCserve HA sur un serveur IIS de Microsoft.

Configurations pour la haute disponibilité d'IIS

Pour implémenter les procédures de haute disponibilité à l'aide du serveur IIS CA ARCserve HA, vous devez disposer des configurations ci-dessous.

- Deux serveurs exécutant Windows Server 2003 ou 2008 :
  - Les deux serveurs doivent disposer du même niveau de Service Packs et de correctifs.
  - Les deux serveurs doivent résider dans la même forêt Active Directory et être membres du même domaine ou de domaines sécurisés.
- Une instance du serveur Microsoft IIS 6.0 ou 7.0 doit être installée sur chaque serveur.
  - Les mêmes services IIS doivent être installés sur les deux serveurs : WWW, SMTP, etc.
  - Les mêmes extensions de services Web doivent être installées sur les deux serveurs.
  - Les chemins complets contenant les fichiers site doivent être identiques sur les deux serveurs.

- Le serveur en attente doit disposer d'une installation propre d'IIS avec les sites par défaut uniquement.
- Les sites du serveur maître ne doivent pas utiliser la redirection des URL ou la redirection du chemin UNC.
- Si un accès anonyme est activé et utilisé, configurez les éléments suivants.

  Pour que les autorisations restent synchronisées entre les deux serveurs, les deux processus IIS doivent utiliser le même compte d'utilisateur pour un accès en tant qu'utilisateur anonyme. Créez un nouveau compte d'utilisateur de domaine et configurez les deux serveurs IIS pour qu'ils utilisent ce compte. Les documents suivants fournissent des explications sur la manière de procéder.

  - Pour IIS 6.0 : *Comment faire : Configuration de l'authentification pour les sites Web IIS dans Windows Server 2003* http://support.microsoft.com/kb/324274
  - Pour IIS 7.0 : *IIS 7.0 : Configure the Anonymous Authentication Identity (en anglais)* http://technet.microsoft.com/fr-fr/library/cc770966

    Remarque : Bien que les documents ne le mentionnent pas, vous devez modifier la stratégie de groupe locale (ou de domaine) afin d'accorder les droits suivants au compte d'utilisateur : Permettre une connexion locale, Ouvrir une session en tant que job de traitement par lots et Accéder à cet ordinateur à partir du réseau. Veillez par ailleurs à dupliquer toutes les modifications d'autorisations apportées au système de fichiers pour le compte d'utilisateur anonyme d'origine également vers le compte de domaine nouvellement affecté.
- Dans IIS 6.0 et 7.0, si vous définissez de nouveaux pools d'applications sur le serveur maître, vous devez également les définir sur le serveur de réplication.
- Si vous utilisez le chiffrement SSL, consultez les documents MS suivants à propos de la copie du certificat approprié.
  - Pour IIS 6.0 : *Comment charger solde une batterie de serveurs Web en utilisant un certificat SSL dans IIS 6.0 et IIS 5.0* à l'adresse http://support.microsoft.com/kb/313299/fr
  - Pour IIS 7.0 : *Configuration d'IIS 7.0* à l'adresse http://technet.microsoft.com/en-us/library/cc268245.aspx
- Le serveur protégé n'est pas un contrôleur de domaine ou un serveur DNS.
- Si vous utilisez IIS 7.0, le composant IIS 6.0 Management Compatibility doit être installé. Etant donné qu'IIS 6.0 Management Compatibility est désactivé par défaut lorsque vous installez IIS 7.0, vous devez activer cette option pendant le processus d'installation d'IIS 7.0 (page 75).

Compte de connexion pour la haute disponibilité d'IIS

Le compte de connexion au service du moteur CA ARCserve HA doit remplir toutes les conditions de compte ci-dessous.

- Il est membre du groupe Administrateurs de domaine. Si le groupe Administrateurs de domaine n'est pas membre des administrateurs du groupe local de domaine intégré, vous devez utiliser un compte qui le soit.
- Il est membre du groupe d'administrateurs de l'ordinateur local. Si le groupe Administrateurs de domaine n'est pas membre, ajoutez le compte manuellement.

Remarque : Si la stratégie de sécurité de votre société nécessite des autorisations plus précises que celles décrites, contactez le support technique pour obtenir des instructions détaillées. Les remarques spéciales s'appliquent aux serveurs IIS utilisés dans des groupes de travail. Pour plus d'informations, consultez le manuel des opération.

Haute disponibilité du serveur Oracle

Cette section décrit la configuration requise pour exécuter CA ARCserve HA sur un serveur Oracle.

Configurations de la haute disponibilité d'Oracle

Pour implémenter les procédures de haute disponibilité à l'aide du serveur Oracle CA ARCserve HA, vous devez disposer des configurations ci-dessous.

- Deux serveurs exécutant Windows Server 2003 ou 2008 :
  - Les deux serveurs doivent disposer du même niveau de Service Packs et de correctifs.
- Les deux serveurs doivent disposer de la même version d'Oracle, des mêmes Service Packs et des mêmes correctifs.
- Les deux serveurs doivent résider dans la même forêt Active Directory et être membres du même domaine ou de domaines sécurisés.
- Le SID Oracle doit correspondre entre les serveurs maître et de réplication.
- Sur les deux serveurs, assurez-vous que tous les services Oracle normalement lancés au démarrage ont été correctement lancés et sont définis sur Démarrage automatique.
- Le chemin d'accès au répertoire ORACLE_HOME et le chemin d'accès aux fichiers de base de données sur les serveurs maître et de réplication doivent être identiques.

- Pour minimiser le trafic de réplication, un ou plusieurs espaces disque logiques temporaires Oracle sont exclus de la réplication (assurez-vous que la base de données Oracle sur le serveur de réplication est configurée avec les mêmes noms et chemins d'espaces disque logiques temporaires que ceux utilisés sur le serveur maître).
- Sur les deux serveurs, configurez Oracle pour monter la base de données automatiquement au démarrage du service (oradim -edit -sid ORACLE_SID -startmode auto).
- Le serveur protégé n'est pas un contrôleur de domaine ou un serveur DNS.

Sur des systèmes UNIX/Linux, CA ARCserve RHA requiert Oracle Instant Client 32 bits pour prendre en charge les bases de données Oracle. Si ce client n'est pas installé, interrompez l'installation de CA ARCserve RHA, téléchargez Oracle Instant Client sur le site Web d'Oracle et redémarrez de l'installation de CA ARCserve RHA. Si le client est déjà installé, fournissez manuellement le chemin d'installation complet.

Compte de connexion pour la haute disponibilité d'Oracle

Le compte de connexion au service du moteur CA ARCserve HA doit remplir toutes les conditions ci-dessous.

- Il est membre du groupe Administrateurs de domaine. Si le groupe Administrateurs de domaine n'est pas membre des administrateurs du groupe local de domaine intégré, vous devez utiliser un compte qui le soit.
- Il est membre du groupe d'administrateurs de l'ordinateur local. Si le groupe Administrateurs de domaine n'est pas membre, ajoutez le compte manuellement.

Remarque : Si la stratégie de sécurité de votre société nécessite des autorisations plus précises que celles décrites, contactez le support technique pour obtenir des instructions détaillées.

Serveurs Oracle fonctionnant dans un groupe de travail

Pour les serveurs d'un groupe de travail, définissez le compte de service du moteur pour un utilisateur membre du groupe d'administrateurs locaux. Les serveurs d'un groupe de travail peuvent utiliser la redirection du système DNS uniquement avec les serveurs DNS qui autorisent les mises à jour non sécurisées. Vous pouvez utiliser normalement le transfert IP, la permutation du nom de l'ordinateur et les scripts de redirection personnalisés.

Réplication et haute disponibilité pour serveurs Microsoft Hyper-V

Réplication pour serveurs Hyper-V

Cette section décrit les conditions requises pour l'exécution de CA ARCserve RHA sur un serveur Hyper-V.

Configuration de la réplication pour Hyper-V

Pour implémenter la réplication pour un serveur Hyper-V, les configurations suivantes sont requises :

- L'ordinateur maître fonctionnant sous Windows Server 2008
- L'ordinateur de réplication fonctionnant sous Windows Server 2003 ou 2008
- Une instance de Hyper-V Server installée sur l'ordinateur maître

Compte de connexion pour la réplication Hyper-V

Le compte de connexion au service du moteur CA ARCserve RHA doit remplir toutes les conditions suivantes :

- Pour les serveurs autonomes (c'est-à-dire ceux qui ne sont pas en cluster), utilisez le compte par défaut du système local.
- Pour les noeuds de cluster, utilisez un compte de service ayant le rôle d'administrateur local sur tous les noeuds de cluster.

Haute disponibilité pour Hyper-V

Cette section décrit la configuration requise pour exécuter CA ARCserve HA sur un serveur Hyper-V.

Configuration de la haute disponibilité pour Hyper-V

Pour implémenter les procédures de haute disponibilité du serveur Hyper-V, vous devez disposer des configurations suivantes.

- Deux serveurs exécutant Windows Server 2008, avec le même niveau de Service Pack et de correctifs
- Les deux serveurs doivent disposer de la même version de Hyper-V, des mêmes Service Packs et des mêmes correctifs.
- Les deux serveurs doivent résider dans la même forêt Active Directory et être membres du même domaine ou de domaines sécurisés.
- Affectez statiquement toutes les adresses IP. Les adresses IP affectées par le serveur DHCP sur le serveur maître ou de réplication ne sont pas prises en charge.
- Le serveur protégé n'est pas un contrôleur de domaine ou un serveur DNS.

N'utilisez pas le chemin d'installation d'Hyper-V par défaut. Créez plutôt un nouveau dossier, tel que c:\vm\ sur l'ordinateur maître et l'ordinateur de réplication. CA ARCserve RHA ne peut pas accéder au chemin d'installation de l'ordinateur virtuel par défaut pendant la détection automatique.

Compte de connexion pour la haute disponibilité de Hyper-V

Le compte de connexion au service du moteur CA ARCserve HA doit remplir toutes les conditions de compte ci-dessous.

- Il est membre du groupe Administrateurs de domaine. Si le groupe Administrateurs de domaine n'est pas membre des administrateurs du groupe local de domaine intégré, vous devez utiliser un compte qui le soit.
- Il est membre du groupe d'administrateurs de l'ordinateur local. Si le groupe Administrateurs de domaine n'est pas membre, ajoutez le compte manuellement.
- Pour les serveurs faisant partie d'un groupe de travail, utilisez le compte du système local.

Réplication et haute disponibilité pour Microsoft SharePoint Server

Réplication pour serveurs SharePoint

Cette section décrit les conditions requises pour l'exécution de CA ARCserve RHA pour les serveurs SharePoint.

Configuration de la réplication pour SharePoint

Pour implémenter la réplication pour un SharePoint Server 2007, les configurations suivantes sont requises :

- Deux serveurs exécutant Windows Server 2003 ou 2008
- Une instance de SharePoint Server installée sur l'ordinateur maître

Pour utiliser la solution de réplication avec l'option de **récupération garantie** pour serveurs SharePoint, vous devez disposer des configurations suivantes :

- La même version de SharePoint Server doit être installée sur les serveurs maître et de réplication.
- SharePoint Server doit être installé avec les mêmes informations d'identification sur les serveurs maître et de réplication.

Compte de connexion pour la réplication pour SharePoint

Le compte de connexion au service du moteur CA ARCserve RHA doit remplir toutes les conditions suivantes :

- Pour les serveurs autonomes (c'est-à-dire ceux qui ne sont pas en cluster), utilisez le compte par défaut du système local.
- Pour les noeuds de cluster, utilisez un compte de service ayant le rôle d'administrateur local sur tous les noeuds de cluster.

Haute disponibilité pour serveurs SharePoint

Cette section décrit la configuration requise pour exécuter CA ARCserve HA sur un serveur SharePoint.

Configuration de la haute disponibilité pour SharePoint

Pour implémenter les procédures de haute disponibilité du serveur SharePoint, vous devez disposer des configurations suivantes.

- Deux serveurs exécutant Windows Server 2003 ou 2008, avec le même niveau de Service Pack et de correctifs
- Une instance de SharePoint Server 2007 installée sur chaque serveur
  - Les deux serveurs doivent disposer des mêmes Service Packs et des mêmes correctifs.
  - Les deux serveurs doivent résider dans la même forêt Active Directory et être membres du même domaine ou de domaines sécurisés.
  - Les deux serveurs doivent utiliser le même port.
  - Une des versions SQL suivantes doit être installée sur les deux serveurs : SQL 2005 SP1 ou ultérieure, SQL 2005 Analysis Services SP1 ou ultérieure.
  - Les deux serveurs doivent disposer de la même version de SQL, des mêmes Service Packs et des mêmes correctifs.
  - Les deux serveurs doivent disposer d'instances SQL Server identiques, à savoir des instances par défaut ou nommées.
  - Les lettres du lecteur contenant les fichiers de base de données doivent être identiques sur les deux serveurs.
  - Le chemin complet de la base de données système par défaut pour chaque instance doit être identique sur les deux serveurs.
- Si vous installez SharePoint avec SQL Server 2005 Express Edition, vous devez activer le protocole TCP/IP pour cette instance SQL (à savoir, OfficeServers) sur les serveurs maître et de réplication.
- Vérifiez que le port défini dans les propriétés TCP/IP de la configuration réseau de la ou des instances SQL est affecté statiquement et qu'il est identique sur l'ordinateur maître et sur l'ordinateur de réplication
- Aucun serveur participant ne peut être contrôleur de domaine ou serveur DNS.
- Les serveurs maître et de réplication doivent se trouver dans la même forêt Active Directory.

Compte de connexion pour la haute disponibilité de SharePoint

Le compte de connexion au service du moteur CA ARCserve HA doit remplir toutes les conditions ci-dessous.

- Il est membre du groupe Administrateurs de domaine. Si le groupe Administrateurs de domaine n'est pas un membre du groupe local de domaines intégré Administrateurs, vous devez utiliser un compte qui soit membre de ce groupe.
- Il est membre du groupe d'administrateurs de l'ordinateur local. Si le groupe Administrateurs de domaine n'est pas membre, ajoutez le compte manuellement.
- Si le compte ne dispose pas d'autorisations d'administration intégrées sur toutes les instances SQL Server, ajoutez les autorisations adéquates.

  Remarques :

  - Vous ne devez pas utiliser de compte de service réseau. Cela peut empêcher les services de fonctionner correctement après une permutation.
  - Si la stratégie de sécurité de votre société nécessite plus d'autorisations précises que celles décrites, contactez le support technique pour obtenir des instructions détaillées. Pour les serveurs d'un groupe de travail, laissez l'utilisateur de la connexion comme système local.

Réplication et Haute Disponibilité pour serveurs vCenter

Réplication pour serveurs vCenter

Cette section décrit les conditions requises pour l'exécution de CA ARCserve RHA pour les serveurs vCenter.

Configuration de la réplication pour vCenter

Pour implémenter la réplication pour les serveurs vCenter, les configurations suivantes sont nécessaires :

- Une instance de vCenter Server installée sur l'ordinateur maître
- Deux serveurs exécutant Windows Server 2003 ou 2008

Pour utiliser la solution de réplication avec l'option de **récupération garantie** pour serveurs vCenter, vous devez disposer des configurations suivantes :

- La même version de vCenter Server doit être installée sur les serveurs maître et de réplication.
- vCenter Server doit être installé avec les mêmes informations d'identification sur les serveurs maître et de réplication.

Compte de connexion pour la réplication pour vCenter

Le compte de connexion au service du moteur CA ARCserve RHA doit remplir toutes les conditions suivantes :

- Pour les serveurs autonomes (c'est-à-dire ceux qui ne sont pas en cluster), utilisez le compte par défaut du système local.
- Pour les noeuds de cluster, utilisez un compte de service ayant le rôle d'administrateur local sur tous les noeuds de cluster.

Haute disponibilité pour serveurs vCenter

Cette section décrit la configuration requise pour exécuter CA ARCserve HA sur un serveur vCenter.

Configuration de la haute disponibilité pour serveurs vCenter

Pour implémenter les procédures de haute disponibilité pour un serveur vCenter, vous devez disposer des configurations ci-dessous.

- Deux serveurs exécutant Windows Server 2003 ou 2008, avec le même niveau de Service Pack et de correctifs
- Les deux serveurs doivent disposer de la même version de vCenter, des mêmes Service Packs et des mêmes correctifs.
- Les deux serveurs doivent résider dans la même forêt Active Directory et être membres du même domaine ou de domaines sécurisés.
- Affectez statiquement toutes les adresses IP. Les adresses IP affectées par le serveur DHCP sur le serveur maître ou de réplication ne sont pas prises en charge.
- Aucun serveur participant ne peut être contrôleur de domaine ou serveur DNS.
- Si le serveur de base de données est installé localement ou à distance sur l'ordinateur maître, configurez l'ordinateur de réplication pour qu'il se connecte au même serveur de base de données.
- Si le serveur de licence est installé localement sur l'ordinateur maître, installez une autre instance du serveur de licence sur l'ordinateur de réplication et configurez l'ordinateur de réplication pour qu'il s'y connecte.
- Si le serveur de licence est installé à distance sur l'ordinateur maître, configurez l'ordinateur de réplication pour qu'il se connecte à cette instance.

Compte de connexion pour la haute disponibilité de vCenter

Le compte de connexion au service du moteur CA ARCserve HA doit remplir toutes les conditions de compte ci-dessous.

- Il est membre du groupe Administrateurs de domaine. Si le groupe Administrateurs de domaine n'est pas membre des administrateurs du groupe local de domaine intégré, vous devez utiliser un compte qui le soit.
- Il est membre du groupe d'administrateurs de l'ordinateur local. Si le groupe Administrateurs de domaine n'est pas membre, ajoutez le compte manuellement.

Réplication et haute disponibilité pour Microsoft Dynamics CRM

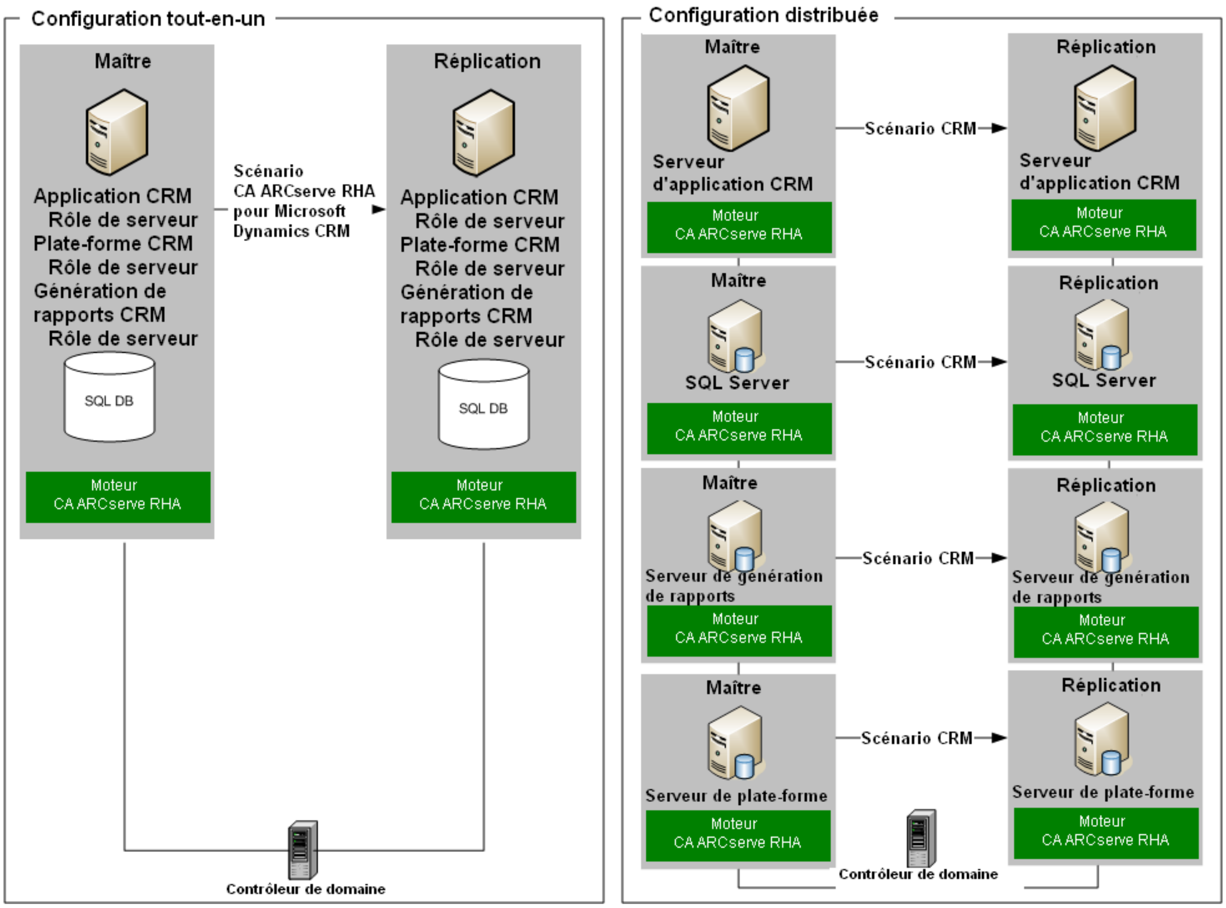
Configuration de Microsoft Dynamics CRM

Microsoft Dynamics CRM est composé de plusieurs rôles de serveur combinés en deux groupes de rôle de serveur :

- Le groupe de rôles de serveur d'application qui contient les services principaux CRM, la Web frontale et l'aide.
- Le groupe de rôles de serveur de plate-forme qui contient le service de traitement asynchrone, le service de détection et le service de génération de rapports.

Les deux groupes de rôles de serveur utilisent le service de génération de rapports de SQL, qui peut être installé sur un ordinateur séparé. Vous pouvez installer des groupes de rôle de serveur sur le même ordinateur ou sur des ordinateurs séparés.

CA ARCserve RHA pour Dynamics CRM peut être configuré de deux façons :



Une configuration tout-en-un

Tous les rôles de groupe de serveurs s'exécutent sur le même ordinateur (serveur maître). Dans une configuration tout-en-un, les éléments suivants sont requis :

- 2 serveurs Windows (maître et de réplication) configurés à l'identique Lorsque vous installez le serveur de réplication, choisissez l'option Etablir une connexion à un déploiement existant. Lorsque vous configurez Dynamics CRM, vous devez choisir l'option Établir une connexion à un déploiement existant, puis entrer l'instance de base de données SQL Server du serveur maître en tant que nom de l'ordinateur qui exécute le serveur SQL à utiliser pour ce déploiement.

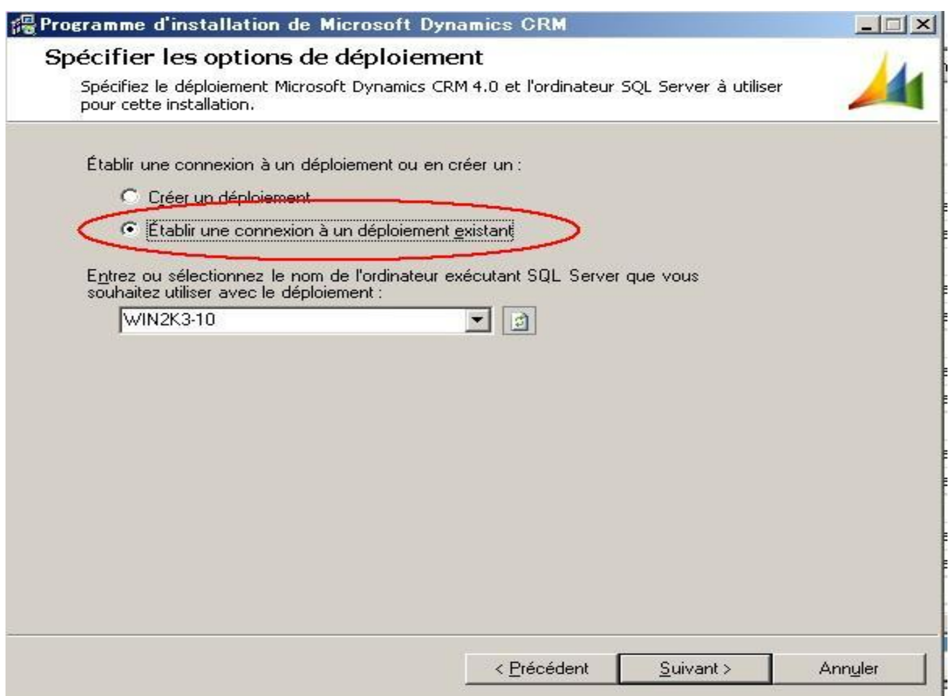
Remarque: Si vous exécutez tous les rôles de serveur sur un ordinateur unique, ce serveur ne peut pas être utilisé en tant que contrôleur de domaine sauf si vous vous exécutez également Microsoft Windows Small Business Server 2003 Premium Edition R2.

Configuration distribuée

Les rôles de groupe de serveurs s'exécutent sur des ordinateurs différents (serveurs maîtres multiples). Dans une configuration distribuée, les éléments suivants sont requis :

- Au moins 2 serveurs Windows (maître et de réplication) utilisés en tant que serveurs d'applications Dynamics CRM, un serveur de plate-forme ou un serveur de génération de rapports Les rôles de serveur d'application, plate-forme et génération de rapports peuvent être assumés par des ordinateurs individuels ou exécutés sur le même ordinateur. Vous pouvez ajouter plusieurs serveurs si nécessaire. Chaque serveur dans le déploiement est protégé par son propre scénario CRM CA ARCserve RHA, donc pour tous les serveurs Dynamics CRM que vous ajoutez, vous devez également ajouter un serveur de réplication configuré à l'identique. Lorsque vous installez le serveur de réplication, choisissez l'option Etablir une connexion à un déploiement existant, puis entrez l'instance de base de données SQL Server du serveur maître en tant que nom de l'ordinateur exécutant le serveur SQL à utiliser pour ce déploiement.
- 2 serveurs SQL : un serveur maître et un serveur de réplication Cet ordinateur est protégé séparément dans un scénario SQL d'arrière-plan. Pour plus d'informations, reportez-vous au *Manuel des opérations pour Microsoft SQL Server* de CA ARCserve RHA.

Remarque: Vérifiez que les services de génération de rapports SQL Server et IIS sont installés avant d'installer Dynamics CRM.



Les règles suivantes s'appliquent :

- Installez le moteur sur tous les serveurs participant à des scénarios CA ARCserve RHA.
- Les deux serveurs Windows doivent exécuter Windows Server 2003 ou 2008 avec le même niveau de Service Pack et de correctifs.
- Le serveur à protéger n'est pas un contrôleur de domaine ou un serveur DNS.

Si vous vous exécutez SQL 2005 dans une configuration distribuée :

- Assurez-vous d'avoir installé une instance SQL sur les deux serveurs (maître et de réplication).
- Assurez-vous que les deux serveurs disposent de la même version de SQL, des mêmes Service Packs et des mêmes correctifs.
- Assurez-vous que les deux serveurs disposent d'instances SQL Server identiques, à savoir des instances par défaut ou nommées.
- Assurez-vous que les deux serveurs se trouvent dans la même forêt Active Directory et qu'ils sont membres du même domaine ou de domaines sécurisés.
- Assurez-vous que les lettres du lecteur contenant les fichiers de base de données sont identiques sur les deux serveurs.
- Assurez-vous que le chemin complet de la base de données système par défaut pour chaque instance est identique sur les deux serveurs.
- Vérifiez que le port défini dans les propriétés TCP/IP de la configuration réseau de l'instance SQL est affecté statiquement et qu'il est identique sur les deux serveurs.

Configuration UNIX/Linux

Sur des serveurs AIX, le nom d'hôte est toujours défini sur FQDN. Lors de la récupération de FQDN, seul DNS est pris en charge. Les services d'attribution de noms NIS ou NIS+ ne sont pas pris en charge.

Si la redirection de système DNS est utilisée, définissez l'ordre de recherche sur l'ordre de liaison, d'hôtes dans /etc/host.conf.

Un package de liaison est requis pour le redirection de système DNS :

Système d'exploitation	**Nom du paquet**
Linux	bind-utils-*
Solaris	SUNWbind

Système d'exploitation	Nom du paquet
AIX	bos.rte.bind_cmds

Pour Oracle sur des systèmes UNIX/Linux, seule l'option de stockage de système de fichiers pour fichiers de données d'instance de base de données est prise en charge.

Haute disponibilité de système complet

La haute disponibilité de système complet peut être configurée comme suit :

Serveur maître

Ce serveur peut être un serveur Windows pris en charge par le moteur et Hyper-V. Le serveur maître peut être un serveur physique ou virtuel.

Serveur de réplication

Ce serveur doit être un serveur Windows 2008 ou Windows 2008 R2 avec le rôle Hyper-V activé. L'UC sur ce serveur doit prendre en charge la virtualisation. Vérifiez que la fonctionnalité est ouverte dans BIOS.

Pour Hyper-V 1.0, vérifiez que tous les patchs sont installés, surtout KB950050. Pour plus d'informations, consultez le site Web de Microsoft.

N'utilisez pas le chemin d'installation par défaut lors de la création d'ordinateur virtuels Hyper-V. CA ARCserve RHA ne peut pas accéder au chemin d'installation de l'ordinateur virtuel par défaut pendant la détection automatique. Créez un nouveau dossier, tel que C:\VM sur l'ordinateur maître et l'ordinateur de réplication. Lors de la création de scénario de haute disponibilité de système complet, spécifiez ce dossier sur la fenêtre de Paramètre des volumes.

Remarque: La haute disponibilité de système complet n'est pas prise en charge sur Windows Server 2000 SP4, car certaines API requises ne sont pas disponibles.

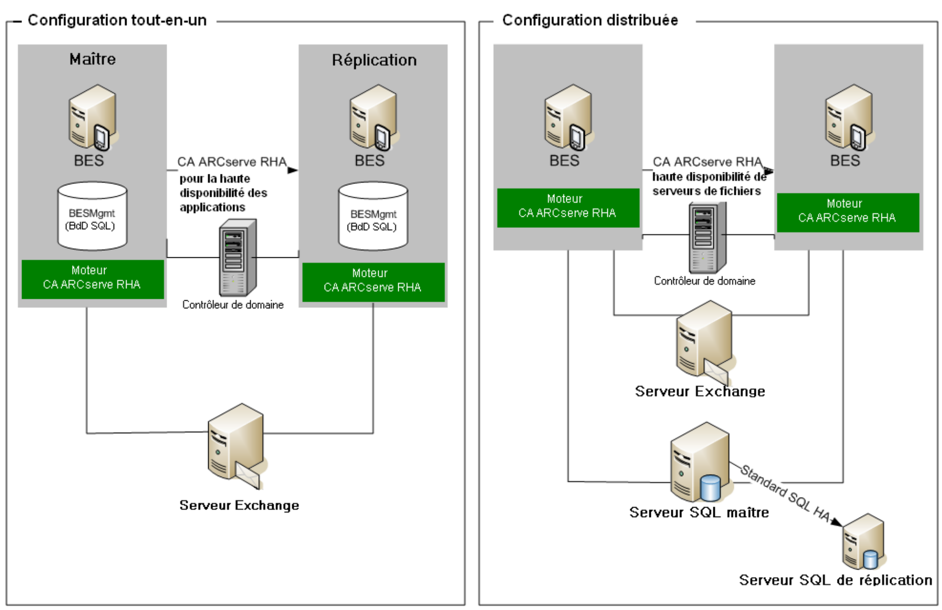
Configuration de BlackBerry pour CA ARCserve RHA

Comme la plupart des administrateurs BlackBerry le savent, les informations de configuration concernant BES sont stockées intégralement ou presque dans la base de données de configuration. Ces informations sont essentielles au bon fonctionnement de BES et constituent également la base d'une permutation réussie par CA ARCserve RHA. La base de données de configuration peut être installée sur le même ordinateur que BES ou sur un ordinateur différent, selon les besoins de votre environnement.

Une installation locale ou sur le même ordinateur crée une dépendance entre SQL et BES, qui sont alors liés sous forme de plate-forme et gérés ensemble, en termes de haute disponibilité, avec CA ARCserve RHA pour les applications. Pour cette raison, nous appelons cette solution la configuration tout-en-un.

Si la base de données SQL est installée sur un ordinateur différent (configuration distribuée), vous pouvez combiner plusieurs scénarios de haute disponibilité afin de décider du niveau de protection à implémenter.

- **Configuration frontale :** créez des scénarios de haute disponibilité de serveur de fichiers modifiés pour utiliser le script de haute disponibilité BlackBerry fourni afin de protéger BES dans des environnements où la base de données SQL séparée est déjà protégée.
- **Configuration d'arrière-plan :** créez des scénarios de haute disponibilité SQL Server standard afin de protéger le serveur SQL séparément de BES. Pour plus d'informations, reportez-vous au Manuel des opérations pour SQL de CA ARCserve RHA.



Dans un environnement comportant deux serveurs BES de production et un seul serveur SQL séparé, vous devez créer trois scénarios de haute disponibilité afin de protéger les six serveurs participant aux scénarios.

Installation sur la configuration et l'installation de CA ARCserve RHA pour BlackBerry

La protection des environnements BlackBerry Enterprise Server avec CA ARCserve RHA requiert une configuration spécifique par étapes. Installez BES sur les serveurs maître et de réplication, configurez les serveurs pour la haute disponibilité, puis connectez la base de données au scénario.

Les procédures d'installation et de configuration complètes sont détaillées dans le *Manuel des opérations pour BlackBerry Enterprise Server de CA ARCserve RHA.*

Haute disponibilité du service de contrôle

Cette section décrit les configurations requises pour l'exécution de la solution de haute disponibilité pour le service de contrôle CA ARCserve RHA.

Important : La solution de haute disponibilité pour le service de contrôle est applicable uniquement à partir de CA ARCserve RHA r12.5 et versions supérieures.

Configuration de la haute disponibilité pour le service de contrôle

Pour implémenter les procédures de haute disponibilité pour le service de contrôle CA ARCserve RHA, les configurations suivantes sont requises :

- Deux serveurs exécutant Windows Server 2003 ou 2008 :
- Une instance d'un service de contrôle doit être installée sur chaque serveur. Les deux instances doivent disposer de la même version du service de contrôle.
- Les deux serveurs doivent disposer des mêmes Service Packs et des mêmes correctifs.
- Les deux serveurs doivent résider dans la même forêt Active Directory et être membres du même domaine ou de domaines sécurisés.
- Les deux serveurs doivent utiliser le même port.
- Aucun serveur participant ne peut être contrôleur de domaine ou serveur DNS.

Compte de connexion de la haute disponibilité pour le service de contrôle

Le compte de connexion au service du moteur CA ARCserve HA doit remplir toutes les conditions ci-dessous.

- Il est membre du groupe Administrateurs de domaine. Si le groupe Administrateurs de domaine n'est pas membre des administrateurs du groupe local de domaine intégré, vous devez utiliser un compte qui le soit.
- Il est membre du groupe d'administrateurs de l'ordinateur local. Si le groupe Administrateurs de domaine n'est pas membre, ajoutez le compte manuellement.

Remarque : Si la stratégie de sécurité de votre société nécessite des autorisations plus précises que celles décrites, contactez le support technique pour obtenir des instructions détaillées.

Annexe A : Installation, mise à niveau et désinstallation de CA ARCserve RHA

Cette section fournit des instructions sur les procédures d'installation et de mise à niveau de CA ARCserve RHA.

Ce chapitre traite des sujets suivants :

Enregistrement de Windows Installer

Pour installer CA ARCserve RHA, le service Microsoft Windows Installer doit être correctement installé et enregistré. Si ce service est arrêté ou endommagé, l'erreur suivante se produit lorsque vous installez ou désinstallez certaines applications :

Windows Installer Error 1720/1722

Il existe deux solutions permettant d'éviter cette erreur.

- Réenregistrez la version du service Windows Installer actuelle.
- Téléchargez la version actualisée du service Windows Installer.

Pour réenregistrer la version actuelle, cliquez sur Démarrer, Exécuter et entrez les commandes suivantes :

```
Msiexec/unregister
```

```
Msiexec/regserver
```

Pour installer la version du service Windows Installer la plus récente :

1. Accédez au site Web de Microsoft et téléchargez la dernière version de Windows Installer.
2. Suivez les instructions de Microsoft pour installer le service selon les conditions requises par votre configuration système.
3. Redémarrez votre ordinateur une fois l'installation terminée.
4. Vérifiez que le service est en cours d'exécution. Cliquez sur Démarrer, Exécuter et entrez la commande suivante :

   ```
   services.msc
   ```

   Si vous exécutez Vista, entrez la commande dans la zone Rechercher.

   La fenêtre Services apparaît. Cherchez le service Windows Installer et vérifiez que le statut est Lancé. Définissez le type de démarrage sur Automatique, si nécessaire, et lancez le service manuellement s'il ne s'exécute pas.

Après avoir installé et vérifié Windows Installer, vous pouvez installer CA ARCserve RHA.

Première installation de CA ARCserve RHA

La première installation des composants CA ARCserve RHA est très simple. Le package d'installation, que vous pouvez télécharger à partir du site Web de CA ARCserve RHA, contient un fichier d'installation appelé Setup.exe. Ce fichier Setup.exe exécute un assistant d'installation standard qui vous guide au cours de l'installation.

- Cette installation n'implique pas de redémarrer ou d'arrêter les applications.
- La version nécessaire de Windows Installer (INSTMSI.EXE) est 3.0. Sauf indication contraire, tous les systèmes d'exploitation pris en charge disposent de Windows Installer 3.0 comme application intégrée.

Des invites standard facilitent l'installation. Votre seule décision importante consiste à choisir les serveurs sur lesquels installer les différents composants.

- Installez le service de contrôle sur un ordinateur utilisé pour surveiller et gérer tous les scénarios.
- Installez le moteur sur les serveurs maître et de réplication.
- L'utilisateur qui installe les composants CA ARCserve RHA doit disposer des droits d'administration locale ou être membre du groupe d'administrateurs locaux.

Le répertoire d'installation par défaut est :
INSTALLDIR\Program Files\CA\ARCServe RHA\noms_composants.

- Au cours de l'installation, vous êtes invité à entrer le compte de service qui exécute le service CA ARCserve RHA.
- Si vous exécutez des scénarios de haute disponibilité, le compte qui exécute le service CA ARCserve RHA peut requérir des droits supplémentaires, en plus de ceux du compte système local (reportez-vous au manuel détaillant le fonctionnement de la haute disponibilité CA ARCserve HA pour plus d'informations).
- Un compte d'utilisateur Windows exécutant le service de contrôle CA ARCserve RHA requiert l'autorisation de lecture et d'écriture sur le répertoire d'installation.
- Le compte de connexion au service pour le moteur CA ARCserve RHA requiert l'autorisation de lecture et d'écriture sur le répertoire d'installation.

Flux de travaux d'installation des composants

L'installation des composants de base CA ARCserve RHA se compose de plusieurs étapes simples.

1. Installation du service de contrôle : installez le service de contrôle sur un serveur Microsoft autonome à l'aide du fichier **Setup.exe**, en sélectionnant l'option **Service de contrôle CA ARCserve RHA** et en suivant les instructions de l'assistant.
2. Installation du gestionnaire : ouvrez la page de présentation de CA ARCserve RHA. Cliquez sur le lien **Gestion des scénarios** sur cette page pour que le système installe automatiquement le gestionnaire CA ARCserve RHA sur votre ordinateur local.
3. Installation des moteurs : ouvrez le gestionnaire et créez un nouveau scénario à l'aide de l'assistant de création de scénarios. Lors de la création du scénario, le système vous autorise à installer le moteur sur les hôtes maître et de réplication qui participent au scénario. Vous pouvez également installer un moteur en local grâce au fichier **Setup.exe**, ou encore installer plusieurs moteurs simultanément à l'aide du programme d'installation à distance.

Mise à niveau d'une installation

Même si CA ARCserve RHA contient de nombreuses différences par rapport à la version antérieure, aucune différence majeure n'existe entre une nouvelle installation et la mise à jour d'une installation existante. Le système détecte automatiquement les composants antérieurs et l'assistant MSI effectue toutes les tâches requises pour mettre à niveau l'application. La plupart des composants d'une version antérieure peuvent rester sur votre réseau. Vous pouvez également importer des scénarios existants et les réutiliser par le biais du gestionnaire CA ARCserve RHA.

Remarque : Les scénarios créés avec la version antérieure ont été enregistrés par défaut dans *INSTALLDIR:\Program Files\CA/ARCserve RHA\ws_scenarios*. Pour plus d'informations concernant le processus d'importation, reportez-vous au *Manuel d'administration de CA ARCserve RHA*.

Pour réussir la mise à niveau, le moteur CA ARCserve RHA antérieur est le seul composant que vous devez supprimer. Par conséquent, vous devez désinstaller CA ARCserve RHA pour chaque serveur maître et de réplication. Vous pouvez utiliser le fichier Setup.exe pour automatiser cette procédure ou la réaliser manuellement avant de lancer la nouvelle installation.

Remarque : Si vous tentez d'installer le service de contrôle sur un ordinateur doté d'une interface utilisateur graphique d'une version précédente, vous obtenez le message ci-dessous.

Une version antérieure de CA ARCserve RHA a été détectée. Vous n'avez pas besoin de la supprimer pour installer la nouvelle version.

Cliquez sur **OK** pour poursuivre l'installation.

Pour supprimer un ancien moteur grâce au fichier setup.exe :

1. Double-cliquez sur le fichier d'installation **Setup.exe**. L'assistant d'installation de CA ARCserve RHA s'affiche.
2. Cliquez sur l'option **Installer**. La page **Installation des composants** s'affiche.
3. Cliquez sur l'option **Installer le moteur CA ARCserve RHA**. Cliquez sur l'option **Installer le moteur CA ARCserve RHA**.

   La boîte de dialogue **Choix de la langue d'installation** s'affiche.
4. Dans la liste déroulante, sélectionnez la langue de l'assistant d'installation de votre choix, puis cliquez sur **OK**.

   Une barre d'avancement s'affiche.
5. Une fois le processus initial terminé, la page **Bienvenue** s'affiche.
6. Cliquez sur **Suivant**. Le système détecte l'existence d'un ancien moteur sur votre serveur ; la page **Informations sur la version précédente** s'affiche alors.
7. Pour supprimer automatiquement le moteur antérieur, cliquez sur **Suivant**. Une barre d'avancement s'affiche.
8. Une fois le processus de suppression terminé, la page **Contrat de licence** apparaît.
9. Suivez les instructions de l'assistant pour terminer l'installation, comme indiqué à la section Installation du moteur CA ARCserve RHA *(page 63).*

Mise à niveau par étapes

Cette version de CA ARCserve RHA est rétrocompatible avec la version précédente, vous pouvez donc la mettre à niveau ultérieurement.

Pour exécuter CA ARCserve RHA dans un environnement mixte, considérez les points suivant :

- Mettez d'abord à niveau le service de contrôle.
- Si vous n'envisagez pas de mettre à niveau les serveurs maître et de réplication en même temps, mettez d'abord à niveau le serveur maître, puis le serveur de réplication. La réplication inverse est prise en charge uniquement si les deux serveurs sont mis à niveau.
- Pour des scénarios de haute disponibilité, vous devez mettre à niveau les serveurs maître et de réplication en même temps.
- Vous ne pouvez pas créer de nouveau serveur de fichiers ou de scénarios d'application lors de l'exécution d'une version plus ancienne du moteur, mais vous pouvez créer de nouveaux scénarios de CD.

Application de proxy XONET

L'application de proxy XONET est un service TCP/IP qui permet à des versions antérieures et actuelles de moteurs CA ARCserve RHA de se trouver sur le même port de réseau. Utilisez-la lorsque vous souhaitez mettre progressivement à niveau une grande base d'installation de distribution de contenu. Consultez la rubrique, Désinstallation des applications v4 et de proxy pour supprimer la version précédente.

La configuration XONET est automatiquement effectuée pendant le processus de mise à niveau. Lorsque vous installez la mise à niveau sur un autre port, XONET surveille le port 25000 et analyse les connexions entrantes. Toutes les connexions v4 sont routées vers le port 24000 (par défaut) et toutes les connexions pour la version actuelle sont routées vers le port 26000 (par défaut).

Pour plus d'informations, consultez la rubrique, Améliorations du programme d'installation.

Remarque : Le proxy XONET prend uniquement en charge les plates-formes Windows.

Package InstallShield

Le package InstallShield de CA ARCserve RHA a été amélioré et inclut désormais une option v4 de conservation permettant de prendre en charge les plans de mise à niveau par étapes. Activez cette option pour conserver les anciennes installations lors de l'installation de la version actuelle de CA ARCserve RHA. Le programme d'installation modifie les paramètres du port actuel (24000) stockés dans le fichier ws_rep.cfg pour la version 4 et installe le fichier ws_rep.cfg incluant un nouveau paramètre de port (26000).

Le programme d'installation à distance prend également en charge les installations conservant la version 4. Lors de la vérification d'un scénario, le programme d'installation à distance détecte les versions de tous les produits CA ARCserve RHA installés sur l'ordinateur cible. Lorsque la version 4 est détectée, une option supplémentaire apparaît dans la boîte de dialogue Paramètres d'installation. Cette option (Désinstaller le moteur version 4 avant la mise à niveau) est activée par défaut. Si vous souhaitez conserver la version 4, désactivez la case à cocher pour afficher des champs supplémentaires. Vos scénarios v4 sont automatiquement importés et convertis.

Important : Si vous installez le proxy XONET sur un cluster Microsoft, vous devez également installer le correctif T5LT025 ou le proxy ne fonctionnera pas. Pour obtenir le correctif, contactez le support.

Port de la version 4

Il s'agit du numéro de port qui sera utilisé pour le moteur de la version 4. Ne modifiez pas la valeur par défaut 24000.

Port de proxy

Il s'agit du numéro de port d'écoute de l'application du proxy XONET. Ne modifiez pas la valeur par défaut 25000.

Numéro de port

Il s'agit du numéro du port d'écoute de la version actuelle du moteur. Ne modifiez pas la valeur par défaut 26000.

Le programme d'installation permet également de réaliser les tâches suivantes :

- Migre tous les utilisateurs de sécurité v4 déléguée dans les groupes de sécurité déléguée correspondant à la version actuelle
- Importation des scénarios créés avec la version précédente et conversion de ces derniers sous la version actuelle
- Possibilité de désinstaller la version 4 et les applications de proxy

Remarque: L'installation de proxy est automatiquement effectuée pendant la mise à niveau. Aucun fichier exécutable n'est disponible séparément.

Désinstallation de la version 4 et des applications de proxy

Vous pouvez désinstaller manuellement la version 4 et les applications de proxy, sur chaque serveur.

Pour désinstaller la version 4 et les applications de proxy :

1. Arrêtez le service de proxy XONET à l'aide de l'applet Services.
2. Pour supprimer le service, exécutez le service de proxy XONET à l'aide du commutateur -uninstall.
3. Supprimez l'application de proxy XONET du disque, si nécessaire.
4. Désinstallez WANsync v4 via l'option Ajout/Suppression de programmes du panneau de configuration Windows.
5. Définissez le paramètre de port dans ws_rep.cfg pour la version actuelle sur 25000.
6. Redémarrez le moteur à l'aide de l'applet Services.

Proxy XONET de dépannage

Symptôme :

Je ne peux pas accéder au moteur de l'interface utilisateur (il apparaît comme déconnecté).

Solution<nbs />:

Effectuez les opérations suivantes :

1. Vérifiez que le service de moteur est activé et en cours d'exécution (accédez à l'applet de services et vérifiez le statut du moteur).
2. Vérifiez que le service de proxy est activé et en cours d'exécution (accédez à l'applet de services et vérifiez le statut du service CAXOProxy).
3. Vérifiez que les ports de moteur pour v4 et pour les versions actuelles correspondent à la configuration de ports de service de proxy. Configuration de ports de proxy par défaut (accédez à l'applet de services et double-cliquez sur entrée de service de proxy. Vérifiez les paramètres du champ d'emplacement de l'exécutable).
    a. Port de proxy principal 25000.
    b. Port de proxy v4 24000 (le port du moteur v4 doit écouter sur ce port ; vérifiez v4 ws_rep.cfg).
    c. Port de proxy de la version actuelle 26000 (le moteur doit écouter sur ce port ; vérifiez ws_rep.cfg).
4. Vérifiez que les scénarios pour v4 et pour la version actuelle font référence au port de proxy principal (dans Scénario, options du moteur, le port du moteur doit être défini sur la valeur par défaut de port de proxy principal (25000).

Installation du service de contrôle CA ARCserve RHA

Cette section décrit l'installation du service de contrôle CA ARCserve RHA.

Remarques concernant l'installation du service de contrôle

Selon le type de procédure à effectuer sur le service de contrôle en lui-même, vous devez installer soit un, soit deux services de contrôle.

- Pour des opérations standard de réplication et de haute disponibilité CA ARCserve RHA, l'installation d'un service de contrôle (page 56) suffit. Ce service de contrôle servira de point de contrôle unique pour toutes les opérations de CA ARCserve RHA. Si vous voulez répliquer les données du service de contrôle SANS effectuer de permutation entre deux services de contrôle, vous pouvez également installer un seul service de contrôle.

  Remarque : Pour répliquer les données du service de contrôle, vous devez créer un scénario de service de contrôle de réplication à l'aide du gestionnaire, une fois l'installation de tous les composants CA ARCserve RHA terminée.

- Pour répliquer les données du service de contrôle et permuter les rôles entre le service de contrôle d'origine et un service de contrôle en attente, vous devez installer deux services de contrôle (page 60). Dans ce cas, un des services de contrôle installés sert de service de contrôle actif, alors que l'autre sert de service de contrôle en attente. Pour installer deux services de contrôle, vous devez répéter le processus d'installation. En effet, vous pouvez installer un seul service de contrôle à la fois.

  Remarques :

  - Pour appliquer la solution de haute disponibilité au service de contrôle, vous devez créer un scénario de service de contrôle de haute disponibilité à l'aide du gestionnaire, une fois l'installation de tous les composants CA ARCserve RHA terminée.
  - Pour appliquer la solution de haute disponibilité au service de contrôle, il n'est PAS nécessaire de détenir une licence de haute disponibilité. Toutefois, vous devez enregistrer CA ARCserve RHA avant de créer un scénario pour le service de contrôle.
  - Pour plus d'informations sur la création de service de contrôle de scénarios de réplication et de haute disponibilité, reportez-vous au manuel d'administration de *CA ARCserve RHA*.

Installation d'un service de contrôle pour une utilisation standard

Pour installer le service de contrôle CA ARCserve RHA :

1. Double-cliquez sur le fichier d'installation **Setup.exe**. L'assistant d'installation de CA ARCserve RHA s'affiche.
2. Cliquez sur l'option **Installer**. La page **Installation des composants** s'affiche.

3. Cliquez sur l'option **Installer le service de contrôle CA ARCserve RHA**. La boîte de dialogue **Choix de la langue d'installation** s'affiche.
4. Dans la liste déroulante, sélectionnez la langue de l'assistant d'installation de votre choix, puis cliquez sur **OK**.

   Une barre d'avancement s'affiche. Une fois le processus initial terminé, la page **Bienvenue** s'affiche.
5. Cliquez sur **Suivant**. La page **Contrat de licence** s'affiche.
6. Sélectionnez la case à cocher **J'accepte** et cliquez sur **Suivant**. La page **Informations client** apparaît.
7. Vérifiez l'exactitude des informations contenues dans les champs et modifiez-les, le cas échéant. Cliquez ensuite sur **Suivant**. La page **Dossier cible** s'affiche.
8. Choisissez l'emplacement d'installation du service de contrôle à l'aide du bouton **Modifier** ou conservez l'emplacement par défaut. Cliquez ensuite sur **Suivant**.

   Remarque : Le répertoire d'installation par défaut est *Program Files\CA\ARCserve RHA\nom_composant.* Tous les fichiers exécutables, DLL et fichiers de configuration se trouvent dans le répertoire INSTALLDIR.

   La page **Configuration SSL** apparaît.
9. La page **Configuration SSL** vous permet d'utiliser un certificat SSL pour sécuriser la communication avec le service de contrôle.

   Si, dans votre environnement informatique, le logiciel est déployé sur un réseau local ne présentant aucun problème de sécurité, vous pouvez désactiver la case **Utiliser la configuration SSL.** La communication avec le service de contrôle se déroule alors sur HTTP.

   Si vous souhaitez utiliser la configuration SSL, sélectionnez la case à cocher **Utiliser la configuration SSL**. Dans ce cas, la communication avec le service de contrôle se déroule sur HTTPS. Après avoir sélectionné cette option, vous devez indiquer un numéro de port dans la case **Port SSL** et entrer un fichier de certificat dans l'une des zones de saisie disponibles.

   Remarques :

   - Lors de la sélection de l'option **Configuration SSL**, le numéro par défaut du **Port SSL** est **443**. Si, toutefois, ce numéro de port est déjà utilisé dans votre environnement informatique, utilisez un autre port.
   - Si vous sélectionnez l'option **Configuration SSL** dans la page de présentation, vous devrez utiliser le nom d'hôte de l'ordinateur du service de contrôle, et non son adresse IP. Saisissez le nom d'hôte et le numéro de port du service de contrôle selon le modèle suivant : https://nom_hôte:numéro_port/page_démarrage.aspx

- Les certificats .CER et .PEX sont des fichiers de sécurité Internet fournis par une autorité de certification tierce. Ces certificats sont installés sur un serveur Web pour authentifier la validité d'un site Web donné, hébergé sur le serveur. Ils sont représentés par une icône en forme de cadenas, près du bord de la fenêtre du navigateur, lors de l'accès à un site sécurisé (qui commence par "https://"). Après avoir saisi le chemin d'accès et le nom d'un certificat .CER ou .PEX dans la page Configuration SSL, l'assistant InstallShield du service de contrôle CA ARCserve RHA installe le certificat et ajoute les métadonnées de certificat SSL sur le serveur Web. De telles métadonnées sont conservées par l'API HTTP dans un métamagasin et utilisées pour localiser les certificats en cas d'échange de certificats lors de sessions HTTPS.
- Si vous ne disposez pas actuellement d'un certificat SSL agréé, vous pouvez utiliser le **Certificat autosigné**. Après avoir sélectionné le bouton d'option **Certificat autosigné**, si vous tentez d'accéder à la page de présentation à partir d'un ordinateur distant, vous devrez installer le certificat. Pour plus d'informations, reportez-vous à la section Installation d'un certificat SSL autosigné (page 79).

10. Cliquez sur **Suivant**. La page **Informations de connexion au service** s'affiche.
11. Faites votre choix et saisissez les informations requises. Vous pouvez utiliser les droits liés au compte du système local ou fournir un nom d'utilisateur et un mot de passe sous la forme Domaine/Nom d'utilisateur.

    Remarque : L'exécution du service de contrôle dans un compte de domaine associé à des droits d'administration sur plusieurs ordinateurs permet le déploiement et la connexion à distance au moteur, sans requérir d'authentification sur chacun des serveurs.
12. Cliquez sur **Suivant**. La page **Rôle du service de contrôle** s'affiche.

    Remarque : Seulement si vous voulez installer deux services de contrôle pour la permutation des rôles (page 60), sélectionnez la case à cocher **Autoriser le service de contrôle** et indiquez si le service de contrôle actuellement installé aura le rôle de service de contrôle **actif** ou de service de contrôle **en attente**.
13. Pour une installation classique du service de contrôle, cliquez sur **Suivant**. La page **Prêt à installer le programme** apparaît.

    Remarque : Cliquez sur le bouton **Précédent** pour revenir aux pages précédentes et modifier votre configuration.
14. Cliquez sur le bouton **Installer** pour installer le service de contrôle. La page **Installation du service de contrôle** apparaît.

15. Une fois l'installation terminée, cliquez sur **Suivant**. La page suivante apparaît.
16. Cliquez sur **Terminer** pour fermer l'assistant. Le service de contrôle est désormais installé à l'emplacement indiqué.

Installation de deux services de contrôle pour la permutation des rôles des services de contrôle

L'installation de deux services de contrôle pour la permutation des rôles est très similaire à l'installation standard. Il existe seulement deux différences principales.

- Pour installer deux services de contrôle, vous devez répéter la procédure d'installation.
- Pendant la procédure d'installation, vous devez indiquer si le service de contrôle que vous installez fonctionnera comme service de contrôle actif ou comme service de contrôle en attente.

Pour installer le service de contrôle pour la permutation des rôles :

1. Double-cliquez sur le fichier d'installation **Setup.exe**. L'assistant d'installation de CA ARCserve RHA s'affiche.
2. Cliquez sur l'option **Installer**. La page **Installation des composants** s'affiche.
3. Cliquez sur l'option **Installer le service de contrôle**. La boîte de dialogue **Choix de la langue d'installation** s'affiche.
4. Dans la liste déroulante, sélectionnez la langue de l'assistant d'installation de votre choix, puis cliquez sur **OK**.

   Une barre d'avancement s'affiche. Une fois le processus initial terminé, la page **Bienvenue** s'affiche.
5. Cliquez sur **Suivant**. La page **Contrat de licence** s'affiche.
6. Sélectionnez la case à cocher **J'accepte** et cliquez sur **Suivant**. La page **Informations client** apparaît.
7. Vérifiez l'exactitude des informations contenues dans les champs et modifiez-les, le cas échéant. Cliquez ensuite sur **Suivant**. La page **Dossier cible** s'affiche.
8. Choisissez l'emplacement d'installation du service de contrôle à l'aide du bouton **Modifier** ou conservez l'emplacement par défaut. Cliquez ensuite sur **Suivant**..

   Remarque : Le répertoire d'installation par défaut (INSTALLDIR) est *\Program Files\CA\ARCserveRHA\component_name*. Tous les fichiers exécutables, DLL et fichiers de configuration se trouvent dans le répertoire INSTALLDIR.

   La page **Configuration SSL** apparaît.
9. La page **Configuration SSL** vous permet d'utiliser un certificat SSL pour sécuriser la communication avec le service de contrôle.
   - Pour utiliser l'option Configuration SSL, reportez-vous à la section Installation d'un service de contrôle pour un fonctionnement standard (page 56).

- Pour utiliser le certificat autosigné SSL, reportez-vous à la section Installation d'un certificat autosigné SSL (page 79).

10. Lorsque vous avez sélectionné la configuration de communication, cliquez sur **Suivant**. La page **Informations de connexion au service** s'affiche.

    Faites votre choix et saisissez les informations requises. Vous pouvez utiliser les droits liés au compte du système local ou fournir un nom d'utilisateur et un mot de passe sous la forme Domaine/Nom d'utilisateur.

    Remarque : L'exécution du service de contrôle dans un compte de domaine associé à des droits d'administration sur plusieurs ordinateurs permet le déploiement et la connexion à distance au moteur, sans requérir d'authentification sur chacun des serveurs.

11. Cliquez sur **Suivant**. La page **Rôle du service de contrôle** s'affiche.

    Pour installer le service de contrôle pour la permutation des rôles, sélectionnez la case à cocher **Autoriser le service de contrôle**. Indiquez ensuite si le service de contrôle actuellement installé assumera le rôle de service de contrôle **actif** ou **en attente**.

12. Cliquez sur **Suivant**. La page **Prêt à installer le programme** apparaît.

    Remarque : Cliquez sur le bouton **Précédent** pour revenir aux pages précédentes et modifier votre configuration.

13. Cliquez sur le bouton **Installer** pour installer le service de contrôle CA ARCserve RHA. La page **Installation du service de contrôle CA ARCserve RHA** apparaît et indique la progression de l'installation.

14. Une fois l'installation terminée, cliquez sur **Suivant**. La page **Fin de l'assistant InstallShield** s'affiche.

15. Cliquez sur **Terminer** pour fermer l'assistant. Le service de contrôle est désormais installé à l'emplacement indiqué.

16. Répétez ce processus d'installation pour le deuxième service de contrôle (actif ou en attente).

17. Installez le moteur CA ARCserve RHA (page 63) sur les serveurs de destination des deux services de contrôle.

Installation du service de contrôle à l'aide de l'interface de ligne de commande

Vous pouvez installer le service de contrôle CA ARCserve RHA à l'aide de l'interface de ligne de commande.

Pour installer le service de contrôle CA ARCserve RHA à l'aide de l'interface de ligne de commande :

- Ouvrez l'interface de ligne de commande et saisissez ce qui suit.

```
CAARCserveRHAManager.exe /S "/v/qn XOLOGIN="[Domain/UserName]"
XOPASSWORD="[Password]" XOLANG="[Language]"
```

Paramètres

CAARCserveRHAManager.exe

Fichier d'installation du service de contrôle de CA ARCserve RHA

S, V, QN

Paramètres d'installation silencieuse

Domaine/Nom d'utilisateur, mot de passe

Entrez les informations requises en fonction de la plate-forme que vous utilisez et de la solution que vous implémentez, tel que décrit dans le chapitre Configuration requise pour les applications et bases de données prises en charge (page 19). Si vous ne saisissez pas les détails du compte de connexion, la valeur par défaut est Système local.

Langue

Sélectionnez la langue de CA ARCserve RHA en utilisant l'un des codes langue suivants :

- "1033" Anglais
- "1036" Français
- "1041" Japonais
- "2052" Chinois (simplifié)
- "1028" Chinois (traditionnel)
- "1031" Allemand
- "1034" Espagnol
- "1040" Italien
- "1046" Portugais (Brésil)

Remarque : Vous ne pouvez pas utiliser SSL dans l'installation silencieuse du service de contrôle.

Exemple : Installez le service de contrôle à l'aide de l'interface de ligne de commande

```
CAARCserveRHAManager.exe /S "/v/qn XOLOGIN="domain/administrator"
XOPASSWORD="abcd" XOLANG="1033"
```

Procédure d'installation du moteur CA ARCserve RHA

Cette section décrit la procédure d'installation du moteur CA ARCserve RHA.

Trois méthodes permettent d'installer le moteur CA ARCserve RHA.

- Utilisation du fichier **Setup.exe** : installation du moteur sur un hôte à la fois. Cette méthode d'installation permet de détecter automatiquement toute version antérieure du moteur et de le supprimer lors de l'installation du nouveau moteur. Les étapes d'installation sont similaires aux étapes d'installation du service de contrôle, telles que décrites à la section Installation du service de contrôle CA ARCserve RHA.
- Utilisation de l'**assistant de création de scénarios** : installation à distance du moteur sur les hôtes maître et de réplication, lors de la création d'un nouveau scénario.
- Utilisation du **programme d'installation à distance** : installation à distance du moteur sur un ou plusieurs hôtes en même temps, grâce à l'assistant d'installation à distance.

Installation du moteur à l'aide du fichier d'installation Setup.exe

Pour installer le moteur CA ARCserve RHA à l'aide du fichier Setup.exe :

1. Double-cliquez sur le fichier d'installation **Setup.exe**. L'assistant d'installation de CA ARCserve RHA s'affiche.
2. Cliquez sur l'option **Installer**. La page **Installation des composants** s'affiche.
3. Cliquez sur l'option **Installer le moteur CA ARCserve RHA**. La boîte de dialogue **Choix de la langue d'installation** s'affiche.
4. Dans la liste déroulante, sélectionnez la langue de l'assistant d'installation de votre choix, puis cliquez sur **OK**.

   Une barre d'avancement s'affiche. Une fois le processus initial terminé, la page **Bienvenue** s'affiche.
5. Cliquez sur **Suivant**. La page **Contrat de licence** s'affiche.

   Remarque : Si votre serveur dispose d'une version précédente du moteur, la page **Informations sur la version précédente** s'affiche pour vous permettre de désinstaller le moteur.
6. Dans la page **Contrat de licence**, sélectionnez la case à cocher **J'accepte** et cliquez sur **Suivant**. La page **Dossier cible** s'affiche.
7. Vérifiez l'exactitude des informations contenues dans les champs et modifiez-les, le cas échéant. Cliquez ensuite sur **Suivant**. La page **Configuration personnalisée** s'affiche.

   Remarque : Lorsque l'option **Moteur** est sélectionnée, le bouton **Espace** est activé. Cliquer sur ce bouton vous permet de voir l'espace disque requis pour l'installation de la fonction sélectionnée.

8. Cliquez sur **Suivant**. La page **Informations de connexion au service** s'affiche.
9. Entrez les informations requises en fonction de la plate-forme que vous utilisez et de la solution que vous implémentez, tel que décrit dans le chapitre Configuration requise pour les applications et bases de données prises en charge.
   - Pour le serveur de fichiers procédez comme suit :
     - Pour les scénarios de réplication, il suffit d'utiliser le compte système local.
     - Pour les clusters (scénarios de réplication), vous devez utiliser le même compte que le service de clusters ou bénéficier d'autorisations équivalentes.
     - Pour les scénarios de haute disponibilité (y compris les clusters) :
     - Vous devez utiliser un compte disposant des droits d'administration de domaine. Si le groupe Administrateurs de domaine n'est pas un membre du groupe local de domaines intégré Administrateurs, vous devez utiliser un compte qui soit membre de ce groupe.
     - Le compte doit également être membre du groupe Administrateurs de l'ordinateur local. Si le groupe Administrateurs de domaine n'est pas membre, ajoutez le compte manuellement. Pour les serveurs faisant partie d'un groupe de travail, utilisez le compte du système local.
10. Cliquez sur **Suivant**. La page **Prêt à installer le programme** s'affiche.
11. Cliquez sur **Installer**. La page **Installation du moteur CA ARCserve RHA** s'affiche.
12. Une fois l'installation terminée, cliquez sur **Suivant**. La page **Fin de l'assistant InstallShield** s'affiche.
13. Cliquez sur **Terminer** pour achever l'installation.

Installation du moteur à l'aide de l'assistant de création de scénarios

Pour installer le moteur à l'aide de l'assistant de création de scénarios :

1. Dans le menu **Scénario** du gestionnaire CA ARCserve RHA, sélectionnez l'option **Nouveau**.

   L'**assistant de création de scénarios** apparaît.

2. Sélectionnez les options de scénarios appropriées comme suit :
   - Sélectionnez le bouton d'option **Créer un scénario**.
   - Dans la liste déroulante **Groupe**, sélectionnez le groupe auquel vous souhaitez attribuer le nouveau scénario ou entrez le nom d'un nouveau groupe.
3. Cliquez sur **Suivant**. La page **Sélection d'un serveur et d'un type de produit** apparaît.
4. Sélectionnez les options de scénarios appropriées comme suit :
   - Dans la liste **Sélection du type de serveur**, sélectionnez le type de serveur utilisé dans le scénario.
   - Parmi les options de **sélection du type de produit**, sélectionnez **Scénario de haute disponibilité**, en fonction de votre licence.
   - **Remarque** : Pour utiliser les options **Tâches sur l'hôte de réplication**, reportez-vous au *Manuel d'administration CA ARCserve RHA*.
5. Cliquez sur **Suivant**. La page **Hôtes maître et de réplication** apparaît.
6. Entrez les informations suivantes.
   - **Nom du scénario** : acceptez le nom du scénario par défaut ou entrez un nouveau nom pour le scénario.
   - **Nom d'hôte/Adresse IP de l'ordinateur maître** et **Nom d'hôte/Adresse IP de l'ordinateur de réplication** : entrez le nom ou l'adresse IP des hôtes maître et de réplication, ou utilisez le bouton **Parcourir** pour les rechercher.

     Remarque : Lorsque vous créez un scénario de haute disponibilité, nous vous recommandons d'entrer l'adresse IP de l'hôte au lieu de son nom.
   - **Informations d'identification de l'utilisateur pour la vérification des hôtes** : entrez les informations d'identification de l'utilisateur qui vous permettront d'accéder aux hôtes distants sur lesquels les moteurs seront installés.

7. Cliquez sur **Suivant**. La page **Vérification du moteur** s'affiche.

   Remarque : Si la boîte de dialogue **Informations d'identification de l'utilisateur pour la vérification des hôtes** s'affiche, entrez les informations d'identification de l'utilisateur qui vous permettront d'accéder aux hôtes distants sur lesquels les moteurs seront installés.

8. Le système vérifie la connectivité des hôtes maître et de réplication que vous avez sélectionnés à la page précédente. Une fois ces connexions vérifiées, le système s'assure qu'un moteur est installé sur chaque hôte.

   Remarque : Un message d'erreur indique qu'une connexion n'a pas pu être établie vers l'hôte spécifié. Si des erreurs sont signalées, vous ne pouvez pas continuer tant qu'elles ne sont pas résolues.

   Vérifiez qu'un moteur est installé sur les hôtes sélectionnés à l'aide de la colonne **Statut du serveur**.

   - Si tous les hôtes disposent d'une version **installée**, vous pouvez passer à la page suivante.
   - Si l'un des hôtes présente la mention **Non installée** dans la colonne Version actuelle, vous devez installer le moteur sur ce ou ces hôtes.

     Remarque : Si aucun moteur n'est installé sur un des hôtes ou sur les deux et si vous cliquez sur le bouton **Suivant**, le message suivant s'affiche.

     Cliquez sur **Non** pour revenir à la page **Vérification du moteur** et installez le moteur.

9. Sur la page **Vérification du moteur**, cliquez sur le bouton **Installer** pour installer à distance le moteur sur l'hôte sélectionné.

   Remarque : Vous pouvez installer le moteur sur les deux hôtes à la fois. Pour ce faire, sélectionnez les cases à cocher des deux hôtes, puis cliquez sur le bouton **Installer**.

10. Attendez la fin de l'installation et le numéro de version du moteur apparaît dans la colonne **Version actuelle**.

Installation sur les hôtes	Statut du serveur	Version actuelle
☑ 155.35.75.135	Installé	15.0.0.2205
☑ 155.35.75.200	Installé	15.0.0.2202

11. Cliquez sur **Suivant**. Les **Répertoires racines de l'ordinateur maître** s'affichent.

    Terminez la création de scénario en suivant les instructions de l'assistant. Pour plus d'informations sur la création d'un scénario, reportez-vous au *Manuel d'administration de CA ARCserve RHA*).

Installation du moteur à l'aide du programme d'installation à distance

Vous pouvez utiliser l'assistant d'installation à distance pour déployer le moteur, en une seule étape, sur un nombre quelconque de serveurs ou de noeuds de cluster.

Si vous exécutez un pare-feu sur l'ordinateur où envisagez d'installer le moteur, vous devez activer le moteur comme exception pour Windows Management Instrumentation (WMI) dans la liste d'exceptions de pare-feu Windows. Si vous exécutez Windows 2003 ou Windows XP, rendez-vous sur le site Web de MSDN Microsoft et recherchez le document Connecting Through Windows Firewall (connexion via un pare-feu Windows).

Pour installer le moteur à l'aide du programme d'installation à distance :

1. Dans le menu **Outils** du gestionnaire CA ARCserve RHA, sélectionnez **Lancer le programme d'installation à distance**.

   La vue du programme d'**installation à distance** s'ouvre et l'**assistant** du programme d'installation à distance apparaît et affiche la page **Sélection d'hôtes**.

   Remarques :

   - Si le gestionnaire contient actuellement des scénarios, les hôtes qui y participent apparaissent dans le panneau **Hôtes sélectionnés**. Cela vous permet de mettre à jour facilement la version du moteur installée sur ces hôtes.
   - Si vous voulez accéder à d'autres fonctionnalités du gestionnaire lors de l'utilisation du programme d'installation à distance, vous pouvez réduire l'assistant d'installation à distance et le réafficher plus tard. Cet assistant est lié à la vue Moniteur du programme d'installation à distance. Si vous changez de vue, l'assistant est automatiquement réduit.

2. Dans la page **Sélection d'hôtes**, sélectionnez les hôtes sur lesquels vous souhaitez installer le moteur. Vous pouvez sélectionner les hôtes automatiquement et manuellement :

   - Pour détecter automatiquement les hôtes existants dans votre domaine, cliquez sur le bouton **Lancer la détection d'hôtes**. Les hôtes détectés apparaissent dans le panneau **Hôtes détectés**, sur la gauche. Double-cliquez sur un hôte pour le sélectionner. Il s'affiche alors dans le volet **Hôtes sélectionnés**, sur la droite.
   - Pour sélectionner manuellement un hôte, entrez son nom d'hôte ou son adresse IP dans la zone **Nom d'hôte/Adresse IP**, puis cliquez sur **Ajouter**. L'hôte entré apparaît dans le volet **Hôtes sélectionnés**.

   Remarque : En cas d'utilisation de clusters, vous devez installer le moteur sur les deux noeuds physiques.

3. Réitérez la sélection autant de fois que nécessaire. Le moteur sera installé uniquement sur les serveurs apparaissant dans le panneau **Hôtes sélectionnés**.

   Remarque : Pour supprimer des hôtes du volet **Hôtes sélectionnés**, sélectionnez l'hôte et cliquez sur le bouton **Supprimer**.

4. Lorsque votre sélection d'hôtes vous convient, cliquez sur **Suivant**. La page **Informations d'identification de l'utilisateur** apparaît.

5. Définissez le compte d'utilisateur qui permet d'accéder à chaque hôte cible. Vous devez disposer des informations d'identification en tant qu'administrateur local pour tous les hôtes sélectionnés.

   Remarques :

   - Vous devez saisir exactement les mêmes **Informations d'identification de l'utilisateur** que vous avez utilisées pour vous connecter à l'hôte distant.
   - Si vous n'avez pas besoin de fournir une valeur Domaine à l'hôte sélectionné, laissez le champ **Domaine** vide et saisissez "**.**" avant le nom d'utilisateur, comme l'illustre l'exemple ci-dessous.

6. Cliquez sur **Suivant**. La page **Vérification de pré-installation** apparaît.

   Le programme d'installation à distance vérifie automatiquement l'existence, la connectivité et la configuration des serveurs sélectionnés à la page précédente. Une fois le processus de vérification terminé, les résultats s'affichent.

   Remarque : Si le statut d'un serveur est signalé comme Erreur et que vous avez vérifié l'existence et les connexions de ce serveur, vous pouvez le sélectionner de nouveau et cliquer sur le bouton **Vérifier encore**. Le programme d'installation à distance réitère le processus de vérification.

7. Lorsque le statut de tous les serveurs est signalé comme **Non Installé**, cliquez sur **Suivant**.

   Remarque : Si une version antérieure du moteur est signalée comme **Installée**, vous pouvez la désinstaller en cliquant sur le bouton **Désinstaller**. Une fois le processus de désinstallation terminé, cliquez sur **Suivant**.

   La page **Paramètres d'installation** apparaît.

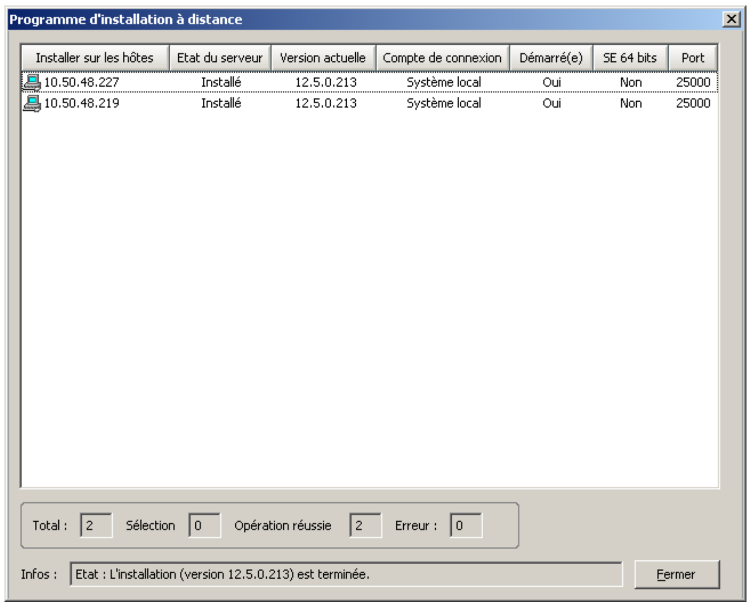
   Dans la section **Informations de connexion au service**, sélectionnez **Ce compte** et entrez le **Domaine\Nom d'utilisateur** et le **Mot de passe** pour définir le compte de connexion pour le service du moteur CA ARCserve RHA.

   Remarque : Sélectionnez la case à cocher **Conserver le compte de connexion au service pour les installations existantes** pour mettre à niveau un moteur existant et pour que CA ARCserve RHA utilise les informations du compte de connexion sous lequel le moteur est installé.

8. Cliquez sur **Suivant**. La page **Prêt pour l'installation** apparaît.

9. Vérifiez que tous les serveurs souhaités sont répertoriés. Puis cliquez sur le bouton **Installer** pour installer le moteur sur ces serveurs. Un message de confirmation s'affiche.

10. Cliquez sur **Oui** pour installer le moteur. Le panneau de statut du **programme d'installation à distance** s'affiche. Attendez que le **statut du serveur** devienne **Installé**.



11. Fermez le volet de statut du **programme d'installation à distance**. Dans la vue du programme d'installation à distance, le statut de l'installation est **Installation terminée** .

    Le moteur est désormais installé sur tous les serveurs ou noeuds de cluster sélectionnés.

Installation du moteur à l'aide de l'interface de ligne de commande

Vous pouvez installer le moteur CA ARCserve RHA sur les serveurs maître et de réplication à l'aide de l'interface de ligne de commande.

Pour installer le moteur CA ARCserve RHA à l'aide de l'interface de ligne de commande :

- Ouvrez l'interface de ligne de commande et saisissez ce qui suit.

```
CAARCserveRHAEngine.exe /S "/v/qn XOLOGIN="[Domain/UserName]"
XOPASSWORD="[Password]" XOPORT="[Port]" XOLANG="[Language]"
```

Paramètres

CAARCserveRHAEngine.exe

Fichier de configuration du moteur CA ARCserve RHA

S, V, QN

Paramètres d'installation silencieuse

Domaine/Nom d'utilisateur, mot de passe

Entrez les informations requises en fonction de la plate-forme que vous utilisez et de la solution que vous implémentez, tel que décrit dans le chapitre Configuration requise pour les applications et bases de données prises en charge (page 19). Si vous ne saisissez pas les détails du compte de connexion, la valeur par défaut est Système local.

Port

Entrez le numéro de port. La valeur par défaut est 25000.

Langue

Sélectionnez la langue en utilisant l'un des codes langue suivants :

- "1033" Anglais
- "1036" Français
- "1041" Japonais
- "2052" Chinois (simplifié)
- "1028" Chinois (traditionnel)
- "1031" Allemand
- "1034" Espagnol
- "1040" Italien
- "1046" Portugais (Brésil)

Exemple : Installer le moteur à l'aide de l'interface de ligne de commande

```
CAARCserveRHAEngine.exe /S "/v/qn XOLOGIN="domaun/administrator"
XOPASSWORD="abcd" XOPORT="25000" XOLANG="1033"
```

Installation et ouverture du centre de gestion et du gestionnaire

Le centre de gestion et le gestionnaire ne requièrent aucune installation préalable de composants ou d'applications. Ils sont basés sur une procédure d'installation simple, réalisable à partir de n'importe quel poste de travail équipé d'une connexion réseau et d'un navigateur Web.

Pour installer le gestionnaire :

1. Ouvrez Internet Explorer. Dans la zone **Adresse**, saisissez le nom d'hôte du service de contrôle ou son adresse IP, puis le numéro de port selon le format suivant : http://nom_hôte:numéro_port/page_démarrage.aspx

   Remarque : Si vous avez sélectionné l'option **Configuration SSL** lors de l'installation du service de contrôle**,** lorsque vous ouvrez la page de présentation, vous devez utiliser le nom d'hôte de l'ordinateur du service de contrôle, et non son adresse IP. Entrez le nom d'hôte du service de contrôle et le numéro de port comme suit : https://nom_hôte:numéro_port/page_démarrage.aspx

   La boîte de dialogue **Connexion** s'affiche.

2. Entrez votre nom d'utilisateur, votre mot de passe et votre domaine, puis cliquez sur **Se connecter**.

3. La **page de présentation** s'affiche.

4. Dans la barre d'outils **Démarrage rapide**, cliquez sur l'option **Gestion des scénarios**.

   La barre de progression qui s'affiche indique que le composant Gestionnaire est en cours d'installation sur l'ordinateur local.

5. Une fois l'installation du gestionnaire terminée, le gestionnaire s'affiche.

   Important : Plusieurs administrateurs peuvent accéder en même temps au gestionnaire CA ARCserve RHA et apporter des modifications si nécessaire, en fonction de leurs droits. La dernière mise à jour apparaîtra comme le dernier état en date du scénario. Ainsi, lorsque plusieurs administrateurs travaillent simultanément dans le gestionnaire, il est important de ne pas oublier qu'un administrateur peut, sans le vouloir, écraser les modifications qu'un autre administrateur vient d'apporter Nous vous recommandons de prendre des mesures internes pour éviter que de tels événements se produisent.

Installation de PowerShell pour CA ARCserve RHA

Cette section décrit l'installation de PowerShell pour CA ARCserve RHA

Pour utiliser PowerShell pour CA ARCserve RHA, vous devez au préalable installer Windows PowerShell. Installez ensuite CA ARCserve RHA PowerShell pour ajouter les composants logiciels enfichables CA ARCserve RHA à l'ensemble de commandes PowerShell.

Important : Les versions de CA ARCserve RHA utilisées pour PowerShell et le service de contrôle auquel il est connecté doivent être identiques.

Pour installer PowerShell pour CA ARCserve RHA :

1. Double-cliquez sur le fichier d'installation **Setup.exe**. L'assistant d'**installation de CA ARCserve RHA** s'affiche.
2. Cliquez sur l'option **Installer**. La page **Installer les composants** s'affiche.
3. Cliquez sur l'option **Installer CA ARCserve RHA PowerShell**. La boîte de dialogue **Choix de la langue d'installation** s'affiche.
4. Dans la liste déroulante, sélectionnez la langue de l'assistant d'installation de votre choix, puis cliquez sur **OK**.

   Une barre d'avancement s'affiche. Une fois le processus initial terminé, la page **Bienvenue** s'affiche.
5. Cliquez sur **Suivant**. La page **Contrat de licence** s'affiche.
6. Sélectionnez la case à cocher **J'accepte** et cliquez sur **Suivant**. La page **Dossier cible** s'affiche.
7. Vérifiez l'exactitude des informations contenues dans les champs et modifiez-les, le cas échéant. Cliquez ensuite sur **Suivant**. La page **Prêt à installer le programme** s'affiche.
8. Cliquez sur **Installer**. Une barre d'avancement s'affiche.
9. Une fois l'installation terminée, cliquez sur Terminer pour achever l'installation.

Désinstallation de CA ARCserve RHA

La désinstallation des composants CA ARCserve RHA est simple et standard, réalisée grâce à l'option **Ajout/Suppression de programmes** du **Panneau de configuration** du système d'exploitation. Vous devez désinstaller chaque composant CA ARCserve RHA séparément.

- La désinstallation ne supprime pas le répertoire par défaut où sont stockés les fichiers de scénario .xmc générés par l'utilisateur et configurés par le gestionnaire CA ARCserve RHA. Il s'agit du répertoire *INSTALLDIR\ ws_scenarios*.
- Il existe deux autres méthodes de désinstallation du moteur CA ARCserve RHA parfaitement adaptées à la désinstallation de versions antérieures du moteur.
  - Utilisation du programme d'installation à distance (page 68)
  - Utilisation du fichier Setup.exe (page 64)

Annexe B : Installation d'IIS 6.0 Management Compatibility pour IIS 7.0

Cette section décrit les étapes nécessaires à l'installation d'IIS 6.0 Management Compatibility pour IIS 7.0. Cette procédure est requise lorsque vous voulez créer un scénario de haute disponibilité pour IIS 7.0.

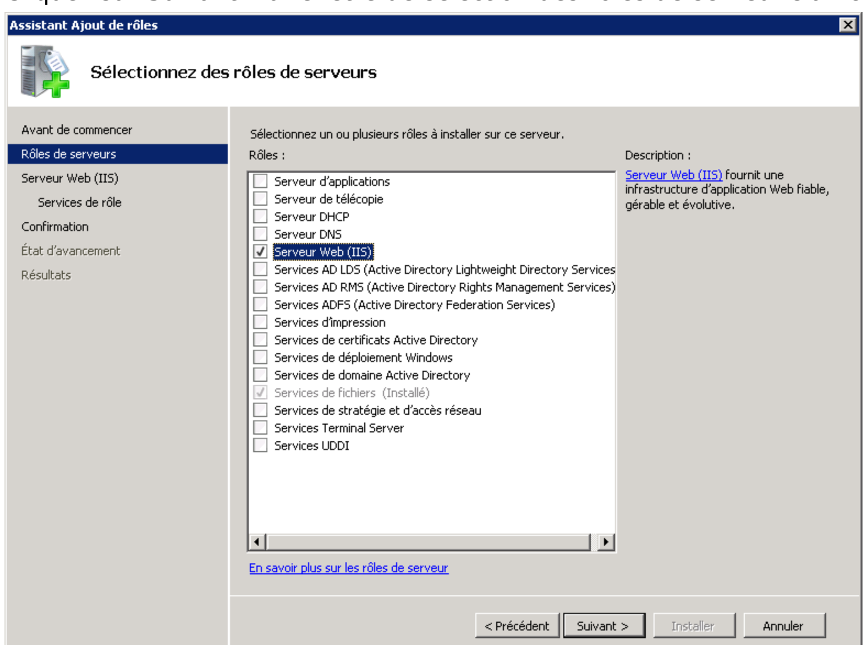
Remarque : Si vous voulez créer un scénario de haute disponibilité pour IIS 7.0, vous devez répéter cette procédure sur l'hôte maître et sur celui de réplication.

Pour installer IIS 6.0 Management Compatibility :

1. Sur l'hôte maître ou sur l'hôte de réplication, ouvrez le gestionnaire de serveurs et sélectionnez l'option Rôles. Cliquez ensuite sur le bouton Ajouter des rôles.

   La première page de l'assistant d'ajout de rôles apparaît.

2. Cliquez sur Suivant. La fenêtre de sélection des rôles de serveur s'affiche.



3. Activez la case à cocher Serveur Web (IIS), puis cliquez sur Suivant.

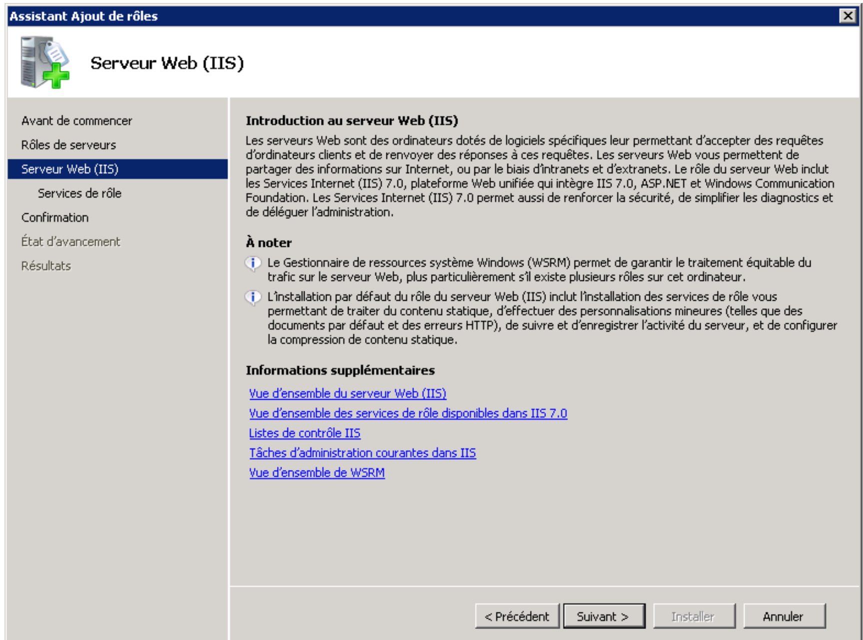
   Un message contextuel s'affiche et vous demande si vous souhaitez ajouter les fonctionnalités requises pour le serveur Web (IIS).

4. Cliquez sur Ajouter les fonctionnalités requises.

La fenêtre de sélection des rôles de serveur s'affiche.

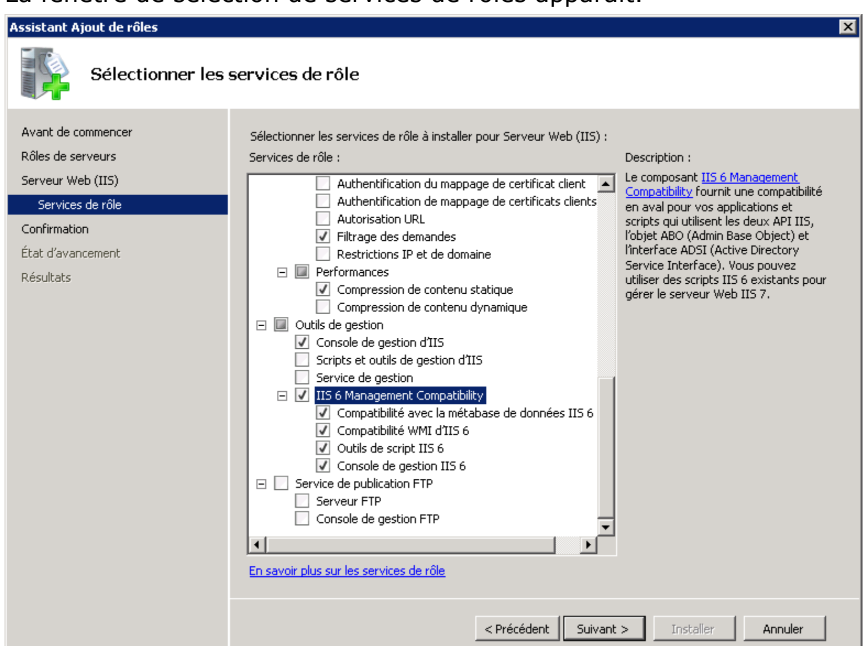
5. Cliquez sur Suivant.

   La fenêtre Serveur Web (IIS) s'affiche.



6. Cliquez sur Suivant.

   La fenêtre de sélection de services de rôles apparaît.



7. Dans la liste des services de rôles, activez la case à cocher IIS 6 Management Capability.
8. Cliquez sur Suivant et suivez les instructions de l'assistant jusqu'à la fin de l'installation.

Annexe C : Installation d'un certificat autosigné SSL

Cette section décrit les étapes nécessaires à l'installation d'un certificat autosigné SSL. Cette procédure est requise lorsque vous utilisez un certificat autosigné pour sécuriser vos communications et que vous tentez de vous connecter au service de contrôle à partir d'un ordinateur distant pour ouvrir la page de présentation.

Installation d'un certificat autosigné

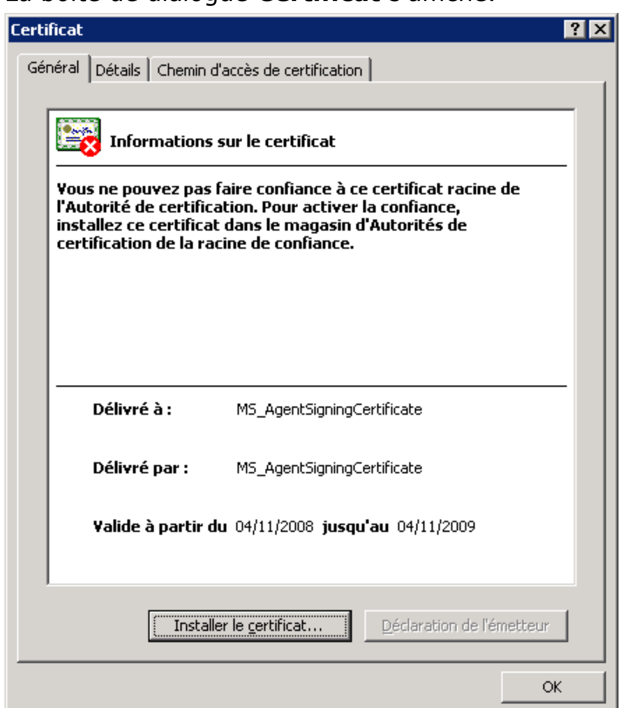
1. Sur l'ordinateur distant, ouvrez Internet Explorer. Dans la zone **Adresse**, saisissez le nom d'hôte du service de contrôle et son numéro de port, comme suit : https://nom_hôte:numéro_port/page_démarrage.aspx

   Remarque : Vous ne pouvez pas utiliser ici l'adresse IP du service de contrôle.

   Une alerte de sécurité apparaît et vous demande si vous souhaitez afficher le certificat.

2. Cliquez sur le bouton **Afficher le certificat**.

   La boîte de dialogue **Certificat** s'affiche.

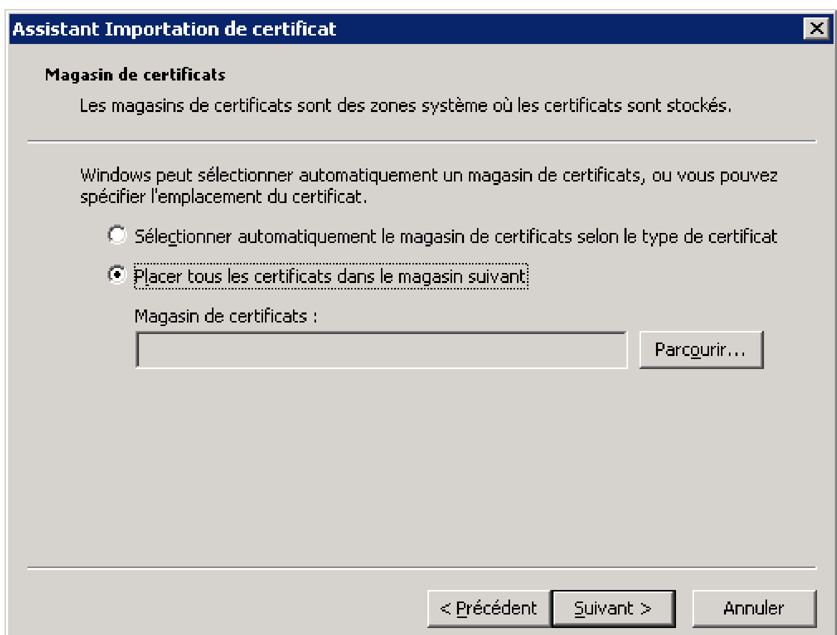


3. Pour installer le certificat en local, cliquez sur le bouton **Installer le certificat**.

   L'**assistant d'importation du certificat** s'affiche.

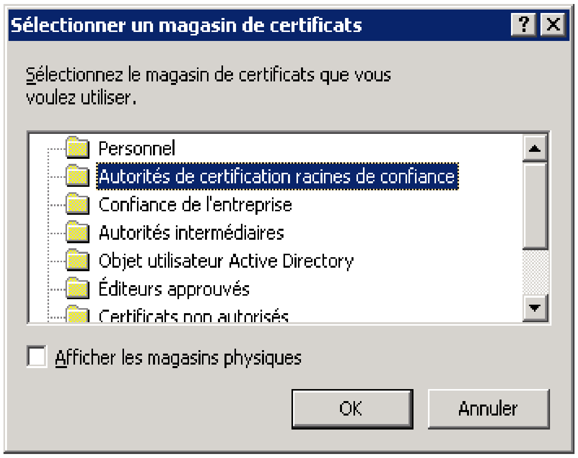


4. Cliquez sur **Suivant**. La page **Magasin de certificats** s'affiche.



5. Sélectionnez le bouton d'option **Placer tous les certificats dans le magasin suivant** et cliquez sur le bouton **Parcourir**.

   La boîte de dialogue **Sélectionner le magasin de certificats** s'affiche.



6. Sélectionnez le magasin **Autorités de certification racines de confiance** et cliquez sur **OK**.

   La page **Terminer l'assistant d'importation de certificats** s'affiche.



7. Cliquez sur **Terminer** pour achever l'importation du certificat.

   Un message de confirmation s'affiche et vous demande de confirmer l'installation du certificat.

8. Cliquez sur **Oui**. Le message qui s'affiche vous informe de la réussite de l'importation.



9. Cliquez sur **OK** pour fermer le message. Cliquez ensuite sur **OK** dans la boîte de dialogue **Certificat** pour la fermer.

   Vous pouvez désormais vous connecter à l'ordinateur du service de contrôle et ouvrir la page de présentation.

Annexe D : Renouvellement d'un certificat SSL expiré

Cette section décrit aux étapes nécessaires pour renouveler un certificat SSL expiré, autorisé ou auto-signé. Cette procédure est requise si vous utilisez déjà un certificat SSL pour sécuriser la communication, si le certificat actuel a expiré et si vous voulez installer un nouveau certificat.

Remarque: Vous ne devez pas arrêter le service de contrôle pendant le processus de renouvellement.

Pour renouveler un certificat SSL expiré :

1. Installez le nouveau certificat obtenu sur l'ordinateur qui exécute le service de contrôle.
2. Pour supprimer l'ancienne liaison de certificat, exécutez la commande suivante :

   ```
   httpcfg.exe delete ssl -i 0,0.0,0:{CS SSL Port Number}
   ```

   Remarque : Le paramètre du **numéro de port SSL CS** correspond au numéro de port saisi pendant l'installation du service de contrôle. Cette valeur figure dans le fichier **ws_man.exe.config**, sous la valeur **ws_port**.

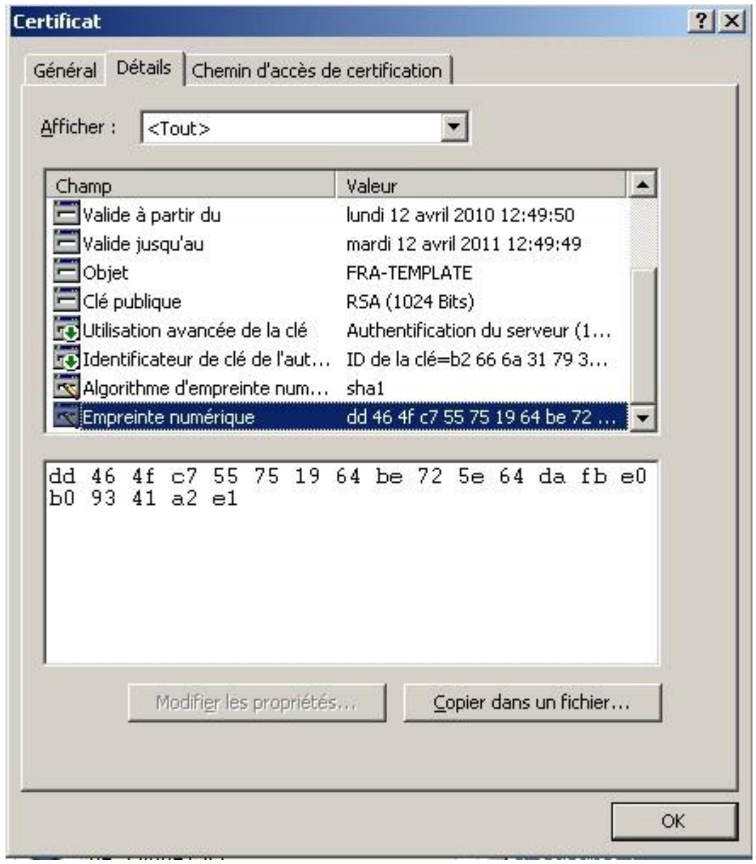
   Le résultat de la commande ne doit indiquer aucune erreur. Le message doit se terminer comme suit :

   ...terminé avec 0.
3. Pour lier le nouveau certificat au port SSL du service de contrôle, exécutez la commande suivante :

   ```
   httpcfg.exe set ssl -i 0,0.0,0:{CS SSL Port Number} -h {New Certificate SslHash}
   ```

Remarques :

- Le paramètre **httpcfg.exe** est un utilitaire Windows Servers standard. Il se trouve dans le répertoire d'installation du service de contrôle.
- Le paramètre du nouveau certificat SslHash se trouve dans l'onglet Détails de la boîte de dialogue Certificat, sous la valeur Empreinte numérique.



N'oubliez pas d'entrer la valeur d'empreinte numérique SANS les espaces entre les caractères. Par exemple : 8f40f9904372ccbd3706d72ed25d.

Le résultat de la commande ne doit indiquer aucune erreur. Le message doit se terminer comme suit :

`...terminé avec 0`.

Le certificat SSL est maintenant renouvelé.

Annexe E : Installation du client Oracle pour la prise en charge d'Oracle 32 bits sur un système d'exploitation 64 bits

Si vous utilisez Oracle 32 bits sur un système d'exploitation 64 bits, vous devez installer la version 11.x ou ultérieure du client Oracle sur l'ordinateur Oracle pour pouvoir exécuter correctement le scénario Oracle.

Pour installer la version 11.x du client Oracle

1. Téléchargez la version 11.x du client Oracle à l'emplacement indiqué ci-dessous.

   http://www.oracle.com/technology/software/tech/oci/instantclient/htdocs/winx64soft.html

2. Installez **Instant Client Package - Basic** dans le répertoire d'installation actuel du moteur ou dans l'un des emplacements par défaut du système d'exploitation.

Annexe F : Notes de fin

Des parties de ce produit comprennent des logiciels développés par des éditeurs tiers. La section ci-dessous contient des informations concernant ces logiciels tiers.

Ce chapitre traite des sujets suivants :

Confirmation ISC bind 9.3.2

Confirmation CAPICOM 2.1.0.1

Ce produit contient une copie de Microsoft CAPICOM 2.1.0.1. Tous les titres, droits et intérêts ci-après sont détenus par Microsoft Corporation.

END-USER LICENSE AGREEMENT MICROSOFT PLATFORM SOFTWARE DEVELOPMENT KIT

IMPORTANT READ CAREFULLY: This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and Microsoft Corporation for the Microsoft software product identified above, which includes computer software and may include associated media, printed materials, and "online" or electronic documentation ("SOFTWARE PRODUCT"). An amendment or addendum to this EULA may accompany the SOFTWARE PRODUCT. YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA BY INSTALLING, COPYING, OR OTHERWISE USING THE SOFTWARE PRODUCT. IF YOU DO NOT AGREE, DO NOT INSTALL OR USE THE SOFTWARE PRODUCT; YOU MAY RETURN IT TO YOUR PLACE OF PURCHASE FOR A FULL REFUND.

1. GRANT OF LICENSE. Microsoft grants you the following rights provided you comply with all terms and conditions of this EULA:

* SOFTWARE PRODUCT. You may install and use an unlimited number of copies of the SOFTWARE PRODUCT on computers, including workstations, terminals or other digital electronic devices residing on your premises ("Computers") to design, develop, and test your software application(s) ("Application") for use with any version or edition of Microsoft Windows 95, Windows 98, Windows NT 4.0, Windows 2000 operating system products and/or any version or edition of any Microsoft operating system product that is a successor to the foregoing and/or any Microsoft product suite that contains any of the foregoing (each a "Microsoft Operating System Product").

* Sample Code. You may modify the sample source code located in the SOFTWARE PRODUCT's "samples" directories ("Sample Code") to design, develop, and test your Application solely for use with a Microsoft Operating System Product. You may also reproduce and distribute the Sample Code in object code form along with any modifications you make to the Sample Code, provided that you comply with the Distribution Terms described below. For purposes of this section, "modifications" shall mean enhancements to the functionality of the Sample Code.

* Redistributable Code. Portions of the SOFTWARE PRODUCT are designated as "Redistributable Code." The text file, \LICENSE\REDIST.TXT, lists the Redistributable code and describes distribution rights associated with the Redistributable Code, subject further to the Distribution Terms specified below.

* Distribution Terms. You may reproduce and distribute an unlimited number of copies of the Sample Code and/or Redistributable Code (collectively "Redistributable Components") as described above in object code form, provided that (a) you distribute the Redistributable Components only in conjunction with and as a part of your Application solely for use with a Microsoft Operating System Product; (b) your Application adds significant and primary functionality to the Redistributable Components; (c) you distribute your Application containing the Redistributable Components pursuant to an End-User License Agreement (which may be "break-the-seal", "click-wrap" or signed), with terms no less protective than those contained herein; (d) you do not permit further redistribution of the Redistributable Components by your end-user customers; (e) you do not use Microsoft's name, logo, or trademarks to market your Application; (f) you include a valid copyright notice on your Application; and (g) you agree to indemnify, hold harmless, and defend Microsoft from and against any claims or lawsuits, including attorneys' fees, that arise or result from the use or distribution of your Application. Contact Microsoft for the applicable licensing terms for all other uses and/or distribution of the Redistributable Components.

* Reservation of Rights. Microsoft reserves all rights not expressly granted to you in this EULA.

* Pre-release code. The SOFTWARE PRODUCT may contain prerelease code that is not at the level of performance and compatibility of the final, generally available, product offering. These portions of the SOFTWARE PRODUCT may not operate correctly and may be substantially modified prior to first commercial shipment. Microsoft is not obligated to make this or any later version of the SOFTWARE PRODUCT commercially available. Microsoft grants you the right to distribute test version of your Application created using the PRERELEASE CODE provided you comply with the Distribution Requirements described in Section 1 and the following additional provisions: (a) you must mark the test version of your Application "BETA" and (b) you are solely responsible for updating your customers with versions of your Application that operate satisfactorily with the final commercial release of the PRERELEASE CODE.

2. CONFIDENTIALITY OF PRERELEASE CODE. The PRERELEASE CODE, including its features, is proprietary and confidential information to Microsoft and its suppliers. you agree not to disclose or provide the PRERELEASE CODE, documentation, or any information relating to the PRERELEASE CODE (including features or the results of use or testing) to any third party except as expressly provided herein without Microsoft's express written permission. However, you may disclose confidential information in accordance with judicial or other governmental order, provided you shall give Microsoft reasonable notice prior to such disclosure and shall comply with any applicable protective order or equivalent. You shall not be liable to Microsoft for such information which you can prove (1) is already known to you; (2) becomes publicly known through no wrongful act of you; (3) is rightfully received from a third party without similar restriction and without breach of this Agreement; or (4) is independently developed by you. This provision shall survive the termination or expiration of this Agreement.

3. TRANSFER Internal. You may move the SOFTWARE PRODUCT to a different Computer. Transfer to Third Party. The initial user of the SOFTWARE PRODUCT may make a one-time transfer of the SOFTWARE PRODUCT to another end user. The transfer has to include all component parts, media, printed materials, this EULA, and if applicable, the Certificate of Authenticity. The transfer may not be an indirect transfer, such as a consignment. Prior to the transfer, the end user receiving the transferred SOFTWARE PRODUCT must agree to all the EULA terms. No Rental. You may not rent, lease, or lend the SOFTWARE PRODUCT.

4. LIMITATION ON REVERSE ENGINEERING, DECOMPILATION, AND DISASSEMBLY. You may not reverse engineer, decompile, or disassemble the SOFTWARE PRODUCT, except and only to the extent that it is expressly permitted by applicable law notwithstanding this limitation.

5. TERMINATION. Without prejudice to any other rights, Microsoft may cancel this EULA if you do not abide by the terms and conditions of this EULA, in which case you must destroy all copies of the SOFTWARE PRODUCT and all of its component parts.

6. CONSENT TO USE OF DATA. You agree that Microsoft and its affiliates may collect and use technical information you provide as a part of support services related to the SOFTWARE PRODUCT. Microsoft agrees not to use this information in a form that personally identifies you.

7. NOT FOR RESALE SOFTWARE. SOFTWARE PRODUCT identified as "Not for Resale" or "NFR," may not be resold, transferred or used for any purpose other than demonstration, test or evaluation.

8. ACADEMIC EDITION SOFTWARE. To use SOFTWARE PRODUCT identified as "Academic Edition" or "AE," you must be a "Qualified Educational User." For qualification-related questions, please contact the Microsoft Sales Information Center/One Microsoft Way/Redmond, WA 98052-6399 or the Microsoft subsidiary serving your country.

9. EXPORT RESTRICTIONS. You acknowledge that the SOFTWARE PRODUCT is of U.S. origin. You agree to comply with all applicable international and national laws that apply to the SOFTWARE PRODUCT, including the U.S. Export Administration Regulations, as well as end-user, end-use and destination restrictions issued by U.S. and other governments. For additional information, see .

10. DISCLAIMER OF WARRANTIES. To the maximum extent permitted by applicable law, Microsoft and its suppliers provide to you the SOFTWARE PRODUCT, and any (if any) support services relating to the SOFTWARE PRODUCT ("Support Services") AS IS AND WITH ALL FAULTS; and Microsoft and its suppliers hereby disclaim with respect to the SOFTWARE PRODUCT and Support Services all warranties and conditions, whether express, implied or statutory, including, but not limited to, any (if any) warranties, duties or conditions of or related to: merchantability, fitness for a particular purpose, lack of viruses, accuracy or completeness of responses, results, workmanlike effort and lack of negligence. ALSO THERE IS NO WARRANTY, DUTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION OR NON-INFRINGEMENT. THE ENTIRE RISK ARISING OUT OF USE OR PERFORMANCE OF THE SOFTWARE PRODUCT AND ANY SUPPORT SERVICES REMAINS WITH YOU.

11. EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND CERTAIN OTHER DAMAGES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL MICROSOFT OR ITS SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, PUNITIVE OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR: LOSS OF PROFITS, LOSS OF CONFIDENTIAL OR OTHER INFORMATION, BUSINESS INTERRUPTION, PERSONAL INJURY, LOSS OF PRIVACY, FAILURE TO MEET ANY DUTY (INCLUDING OF GOOD FAITH OR OF REASONABLE CARE), NEGLIGENCE, AND ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE PRODUCT OR THE SUPPORT SERVICES, OR THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS EULA, EVEN IF MICROSOFT OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

12. LIMITATION OF LIABILITY AND REMEDIES. Notwithstanding any damages that you might incur for any reason whatsoever (including, without limitation, all damages referenced above and all direct or general damages), the entire liability of Microsoft and any of its suppliers under any provision of this EULA and your exclusive remedy for all of the foregoing shall be limited to the greater of the amount actually paid by you for the SOFTWARE PRODUCT or U.S.$5,00. The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails its essential purpose.

13. NOTE ON JAVA SUPPORT. THE SOFTWARE PRODUCT MAY CONTAIN SUPPORT FOR PROGRAMS WRITTEN IN JAVA. JAVA TECHNOLOGY IS NOT FAULT TOLERANT AND IS NOT DESIGNED, MANUFACTURED, OR INTENDED FOR USE OR RESALE AS ONLINE CONTROL EQUIPMENT IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL-SAFE PERFORMANCE, SUCH AS IN THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, AIR TRAFFIC CONTROL, DIRECT LIFE SUPPORT MACHINES, OR WEAPONS SYSTEMS, IN WHICH THE FAILURE OF JAVA TECHNOLOGY COULD LEAD DIRECTLY TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE. Sun Microsystems, Inc. has contractually obligated Microsoft to make this disclaimer.

14. U.S. GOVERNMENT LICENSE RIGHTS. All SOFTWARE PRODUCT provided to the U.S. Government pursuant to solicitations issued on or after 1 décembre 1995 is provided with the commercial license rights and restrictions described elsewhere herein. All SOFTWARE PRODUCT provided to the U.S. Government pursuant to solicitations issued prior to 1 décembre 1995 is provided with "Restricted Rights" as provided for in FAR, 48 CFR 52,227-14 (JUNE 1987) or DFAR, 48 CFR 252,227-7013 (OCT 1988), as applicable.

15. APPLICABLE LAW. If you acquired this SOFTWARE PRODUCT in the United States, this EULA is governed by the laws of the State of Washington. If you acquired this SOFTWARE PRODUCT in Canada, unless expressly prohibited by local law, this EULA is governed by the laws in force in the Province of Ontario, Canada; and, in respect of any dispute which may arise hereunder, you consent to the jurisdiction of the federal and provincial courts sitting in Toronto, Ontario. If this SOFTWARE PRODUCT was acquired outside the United States, then local law may apply.

16. ENTIRE AGREEMENT. This EULA (including any addendum or amendment to this EULA which is included with the SOFTWARE PRODUCT) are the entire agreement between you and Microsoft relating to the SOFTWARE PRODUCT and the support services (if any) and they supersede all prior or contemporaneous oral or written communications, proposals and representations with respect to the SOFTWARE PRODUCT or any other subject matter covered by this EULA. To the extent the terms of any Microsoft policies or programs for support services conflict with the terms of this EULA, the terms of this EULA shall control.

17. The SOFTWARE PRODUCT is protected by copyright and other intellectual property laws and treaties. Microsoft or its suppliers own the title, copyright, and other intellectual property rights in the SOFTWARE PRODUCT. The SOFTWARE PRODUCT is licensed, not sold.

All copyright and other notices contained in CAPICOM must remain in their entirety with such component.

Confirmation Zlib 1.2.3

/* zlib.h -- interface de la bibliothèque de compression universelle "zlib", version 1.1.4, 11 mars 2002

Copyright (C) 1995-2002 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.
Acknowledgement

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

Index

I

M

N

P

R

S

T

W